1   Michael W. Sobol (SBN 194857)
    msobol@lchb.com
2   David T. Rudolph (SBN 233457)
    drudolph@lchb.com
3   Jallé H. Dafa (SBN 290637)
    jdafa@lchb.com
4   John D. Maher (SBN 316157)
    jmaher@lchb.com
5   Nabila Abdallah (SBN 347764)
    nabdallah@lchb.com
6   LIEFF CABRASER HEIMANN
       & BERNSTEIN, LLP
7   275 Battery Street, 29th Floor
    San Francisco, CA 94111
    Telephone: 415.956.1000
8   Facsimile: 415.956.1008

9   *Attorney for Plaintiffs and the Class*

10

11   **UNITED STATES DISTRICT COURT**

12   **NORTHERN DISTRICT OF CALIFORNIA**

13   **SAN FRANCISCO DIVISION**

14

15   Michael Katz-Lacabe and Dr. Jennifer   Case No. 3:22-cv-04792-RS
     Golbeck, on behalf of themselves and all
16   others similarly situated,   **SECOND AMENDED CLASS ACTION**
                                                    COMPLAINT
17   Plaintiffs,
                                                    CLASS ACTION
18   vs.
                                                    DEMAND FOR JURY TRIAL
19   ORACLE AMERICA, INC., a corporation
     organized under the laws of the State of
20   Delaware,

21   Defendant.

22

23

24

25

26

27

28

1

TABLE OF CONTENTS

2

Page

28

1

TABLE OF CONTENTS
(continued)

2

Page

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   **I.   INTRODUCTION**

2   1.   This second amended complaint sets forth how the regularly conducted business

3   practices of defendant Oracle America, Inc. ("Oracle") amount to a deliberate and purposeful

4   surveillance of the general population via their digital and online existence. In the course of

5   functioning as a worldwide data broker, Oracle has created a network that tracks in real time and

6   records indefinitely the personal information of hundreds of millions of people. Oracle sells this

7   detailed personal information to third parties, either directly, or through its "ID Graph" and other

8   related products and services derived from this data. The proposed Classes herein lack a direct

9   relationship with Oracle and have no reasonable or practical basis upon which they could legally

10   consent to Oracle's surveillance.

11   2.   The named Plaintiff class representatives are informed and concerned citizens who

12   believe that the unregulated worldwide data marketplace abrogates the privacy and autonomy of

13   the people and threatens core principles essential for democratic self-rule. Plaintiffs bring this

14   action to enforce their fundamental right to privacy, seek redress and compensation for the

15   financial, dignitary, reputational, and relational harms Oracle has caused, and obtain a ruling that

16   Oracle's conduct is unlawful and therefore must stop. The law, as alleged below, entitles Plaintiffs

17   and the proposed Classes to these remedies.

18   **II.   THE PARTIES**

19   3.   Plaintiff Michael Katz-Lacabe resides in San Leandro, California. Mr. Katz-

20   Lacabe is a privacy rights activist. He is the founder of the Center for Human Rights and Privacy,

21   a project dedicated to the promotion of human rights and privacy in the United States, focusing on

22   the use of surveillance technologies by local police and other government agencies.[1] Mr. Katz-

23   Lacabe is also an active member of Oakland Privacy, a grassroots citizens' coalition that "works

24   regionally to defend the right to privacy and enhance public transparency and oversight regarding

25   the use of surveillance techniques and equipment."[2] Mr. Katz-Lacabe has been frequently cited by

26   [1] *About CEHRP*, The Center for Human Rights and Privacy (2014), https://www.cehrp.org/about-

27   cehrp/ [https://perma.cc/9T3N-ZH5W].
      [2] *About*, Oakland Privacy (2022), https://oaklandprivacy.org/about/ [https://perma.cc/N8VH-

28   5TCH].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                    CASE NO. 3:22-CV-04792-RS

1 reporters for his privacy work related to the use of license plate readers by local police,[3] which has

2 been referenced by advocacy organizations in their California Supreme Court *Amicus Curiae*

3 briefs.[4]

4   4.   Mr. Katz-Lacabe, like most members of modern society, must use the Internet to

5 conduct routine affairs of daily life. On May 4, 2022, despite taking significant steps to maintain

6 his online and offline privacy, Mr. Katz-Lacabe received an "Offline Access Request

7 Response Report" ("OARRR") from Oracle indicating Oracle had tracked, compiled, and analyzed

8 his web browsing, geolocation, brick-and-mortar purchase, and other activity and thereby created

9 an electronic profile on him, attached hereto as Exhibit A.[5] On information and belief, Oracle

10 continues to track Mr. Katz-Lacabe's internet and offline activity, enrich the profile of him as

11 described below, and make his personal information available to third parties without his consent.

12 On information and belief, Mr. Katz-Lacabe has visited websites where his electronic

13 communications were intercepted by the use of Oracle JavaScript code, as described below.

14   5.   The full scope and extent of Oracle's tracking and compiling of Mr. Katz-Lacabe's

15 internet and offline activity and personal data resides with Oracle itself, is not fully disclosed by

16 Oracle, and therefore must be determined through discovery from Oracle. Based on information

17 known at this time, Mr. Katz-Lacabe alleges as follows.

18

19 _____

20 [3] Cyrus Farivar, *Op-Ed: Technology TurnsOour Cities into Spies for ICE, Whether We Like it or Not*, Los Angeles Times (May 2, 2018, 4:15 AM), https://www.latimes.com/opinion/op-ed/la-oe-farivar-surveillance-tech-20180502-story.html [https://perma.cc/89AL-WMA4]*; Cyrus Farivar,

21 *California cities, counties have spent $65M on spy tech in past decade*, Ars Technica (Nov. 12, 2014, 6:45 AM), https://arstechnica.com/tech-policy/2014/11/california-cities-counties-have-

22 spent-65m-on-spy-tech-in-past-decade/ [https://perma.cc/NA4Z-MRV9]; Andy Greenberg & Ryan Mac, *How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut*,

23 Forbes (Aug.14, 2013, 10:10 AM), https://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-

24 philosopher-built-palantir-a-cia-funded-data-mining-

25 juggernaut/?sh=6b9236727785[https://perma.cc/25ZT-BBL6].

[4] *Application for Leave to File Amicus Curiae Brief and Amicus Curiae Brief of Electronic

26 Privacy Information Center (EPIC) in Support of Petitioners*, Supreme Court of the State of California (May 17, 2016), https://www.courts.ca.gov/documents/15-s227106-ac-elec-privacy-

27 info-ctr-051716.pdf [https://perma.cc/PBK6-LDFJ].

[5] Plaintiffs reattach hereto as Exhibits A and B the identical documents previously filed with the

28 Court at Docket No. 84, pursuant to the Court's order on sealing (Dkt. No. 77). The unredacted versions of Exhibits A and B were previously filed with the Court at Docket Nos. 75-2 and 75-3.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   6.   Oracle has tracked Mr. Katz-Lacabe's activity on at least hundreds of websites.

2   Mr. Katz-Lacabe has searched for and viewed articles related to political and personal financial

3   issues on numerous websites. Oracle tracking mechanisms, including "cookies," "pixels," and/or

4   javascript code, as described below at paragraphs 41-59, were present on those websites,

5   including, on information and belief, at the time Mr. Katz-Lacabe accessed them. Those tracking

6   mechanisms transmitted to Oracle the URL data coupled with unique identifiers that Oracle used

7   to associate that browsing history with other data compiled into a data profile about him. On

8   information and belief, the bk-coretag javascript code was present on a subset of websites at the

9   time Mr. Katz-Lacabe read those articles, and that code transmitted to Oracle the URLs for the

10   specific articles and web pages he was reading to Oracle, and also transmitted information he

11   entered into fields on these websites, including but not limited to search terms, as well as add-to-

12   cart actions, and other communications with websites. Oracle maintains a data profile concerning

13   Mr. Katz-Lacabe, which Oracle provides direct access or indirect access (e.g., via products or

14   services derived from the profile) to unknown third parties. On information and belief, Oracle

15   engaged in this conduct throughout the class period. The websites visited by Mr. Katz-Lacabe

16   where Oracle tracking mechanisms have been detected include but are not limited to:

17   a.   abcnews.com

18   b.   citi.com

19   c.   fivethirtyeight.com

20   d.   govdelivery.com

21   e.   ktla.com

22   f.   nasdaq.com

23   g.   nytimes.com

24   7.   Oracle partnered with a company called PlaceIQ to obtain, compile, and analyze

25   hundreds of physical locations Mr. Katz-Lacabe had traveled to, and then made that data, or

26   information derived from that data (such as "segments" described at paragraphs 57, 64, and 74-76

27   below), via products or services derived from that profile available to unknown third parties

28   through its Data Marketplace. According to a press release, "PlaceIQ, the company building a

- 3 -   SECOND AMENDED CLASS ACTION COMPLAINT
               CASE NO. 3:22-CV-04792-RS

1   new model of consumer behavior by connecting physical and digital activities across time, space,

2   and mobile devices," made "PlaceIQ audience data available through Oracle Data Cloud's

3   BlueKai Marketplace," and "[t]his integration gives Oracle Data Cloud users convenient access to

4   PlaceIQ's rich consumer audiences, built from real world movement data and observations."[6]

5   Oracle thus provided unknown third parties with "convenient access" to Mr. Katz-Lacabe's "real

6   world movement data." Mr. Katz-Lacabe was neither aware of nor consented to this conduct. The

7   Center for Digital Democracy has urged the FTC to open an inquiry into Place IQ's practices, as

8   these practices "may lead to new forms of discrimination, as consumers are treated differently

9   based on race, ethnicity, income, etc."[7] Through PlaceIQ, Oracle tracked Mr. Katz-Lacabe's

10   activity at hundreds of specific locations, including:

11   a.   retail locations;

12   b.   restaurants;

13   c.   gas stations;

14   d.   banks—including the specific type of bank and branch, thereby revealing

15   which banks Katz-Lacabe does business with; and

16   8.   Oracle obtained, compiled, and analyzed information about hundreds of Mr. Katz-

17   Lacabe credit card purchases, and then made that data or information derived from that data (such

18   as "segments" described at paragraphs 57, 64, and 74-76 below), via products or services derived

19   from that profile available to third parties through its Data Marketplace. On information and

20   belief, Oracle obtained, and continues to maintain in its systems, information about his credit card

21   purchases, including reflecting specific spending habits and preferences, as well as specific

22   purchase amounts and even SKUs for specific products. For instance, the OARRR states "Oracle

23   Data Cloud collected purchase-related retail data associated with your profile, indicating that you

---

[6] *PlaceIQ Data Now Available Through Oracle Data Cloud's BlueKai Marketplace*, PlaceIQ (July 13, 2016), https://www.placeiq.com/2016/07/placeiq-data-now-available-through-oracle-data-clouds-bluekai-marketplace/ [https://perma.cc/22T8-MVGZ]

[7] U.S. PIRG and the Center for Digital Democracy, Protecting Consumer Privacy and Welfare in the Era of "E-scores," Real-time Big Data "Lead-Generation" Practices and other Scoring/Profile Applications, https://www.democraticmedia.org/sites/default/files/AltScoringCommentsFTC18March14PIRG%26CDD_0.pdf [https://perma.cc/2R97-F7WK].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   spent the following amounts at retail businesses in the last 12 months," and lists a specific

2   purchase for a specific product, including the SKU identifying the product, as well the price Mr.

3   Katz-Lacabe paid for that product. Mr. Katz-Lacabe was neither aware of nor consented to this

4   conduct.

5   9.   The OARRR also demonstrates that Oracle obtained, compiled, and analyzed

6   sensitive information about Mr. Katz-Lacabe's finances and credit, including information about

7   his ability to pay a mortgage, his creditworthiness, and the risks he presents to potential creditors.

8   10.   Oracle associated the above information with a profile through its ID Graph, as

9   described below, that contained detailed demographic information about him, as well as his name,

10 email addresses, physical address, and phone numbers. As such, a person in possession of any of

11 these identifiers, along with access to Oracle's dossier on him, could learn highly detailed,

12 sensitive information about him.

13   11.   Plaintiff Dr. Jennifer Golbeck resides in Sugarloaf Key, Florida. Dr. Golbeck is a

14 Professor at the University of Maryland in College Park and is Director of the Social Intelligence

15 Lab. She is an expert in social networks, social media, privacy, and security on the web. As

16 described in her Wikipedia entry, Dr. Golbeck "is known for her work on computational social

17 network analysis. She developed methods for inferring information about relationships and people

18 in social networks. Her models for computing trust between people in social networks are among

19 the first in the field . . . [Dr.] Golbeck has received attention for her work on computing

20 personality traits and political preferences of individuals based on their social network profiles.

21 Her presentation at TEDxMidatlantic, discussing the need for new methods of educating users

22 about how to protect their personal data, was selected as one of TED's 2014 Year in Ideas talks."[8]

23 Dr. Golbeck's TED talk, "The curly fry conundrum: Why social media 'likes' say more than you

24 might think," has received over 300,000 views on YouTube.[9]

25

26 ───────────────

[8] Wikipedia, *Jen Golbeck*, https://en.wikipedia.org/wiki/Jen_Golbeck [https://perma.cc/7Y2P-
27 SU4C].

[9] TED, *Jennifer Golbeck: The Curly Fry Conundrum: Why Social Media "Likes" Say More Than*
28 *You might Think*, YouTube (Apr. 3, 2014), https://www.youtube.com/watch?v=hgWie9dnssU
    [https://perma.cc/89JD-556N].

SECOND AMENDED CLASS ACTION COMPLAINT
                                        CASE NO. 3:22-CV-04792-RS

1   12.   Dr. Golbeck, like most members of modern society, must use the Internet to

2 conduct routine affairs of daily life. Despite taking precautions to keep her personal information

3 from being collected by third parties, Dr. Golbeck discovered Oracle tracking devices on multiple

4 of her computers that she regularly uses for internet browsing and other activities. Additionally,

5 on March 10, 2022, Dr. Golbeck received from Oracle an OARRR indicating Oracle had tracked,

6 compiled, and analyzed her web browsing, geolocation, brick-and-mortar purchase and other

7 activity and thereby created an electronic profile on her, attached hereto as Exhibit B. On

8 information and belief, Oracle continues to track Dr. Golbeck's internet and offline activity, enrich

9 the profile of her as described below, and make her personal information available to third parties

10 without her consent. On information and belief, Dr. Golbeck visited websites where her electronic

11 communications were intercepted by the use of Oracle JavaScript code, as described below.

12   13.   The full scope and extent of Oracle's tracking and compiling of Dr. Golbeck's

13 internet and offline activity and personal data resides with Oracle itself, is not fully disclosed by

14 Oracle, and therefore must be determined through discovery from Oracle. Based on information

15 known at this time, Dr. Golbeck alleges as follows.

16   14.   Dr. Golbeck has searched for and viewed articles related to sensitive health issues

17 on numerous health-specific websites. On information and belief, the bk-coretag javascript code

18 was present on those websites at the time Dr. Golbeck read those articles, and that code

19 transmitted to Oracle the URLs for the specific articles and web pages she accessed, as well as

20 content she entered in search forms and other fields, add-to-cart actions, and other

21 communications with websites along with a unique identifier that Oracle then used to associate

22 that browsing history with a profile of her maintained by Oracle, which profile Oracle then

23 provided unknown third parties access to. On information and belief, Dr. Golbeck's interest in the

24 subject matter of those articles was made available and sold to those third parties. On information

25 and belief, Oracle engaged in this conduct throughout the class period. Dr. Golbeck. The websites

26 visited by Dr. Golbeck. where Oracle JavaScript tracking mechanisms have been detected include

27 at least:

28   a.   Healthline.com.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

b.   Psychiatry.org

15.   Oracle has tracked Dr. Golbeck's activity on at least hundreds of other websites. Oracle tracking mechanisms, including "cookies," "pixels," and/or javascript code, as described below at paragraphs 41-59, were present on those websites, including, on information and belief, at the time Dr. Golbeck accessed them. Those tracking mechanisms transmitted to Oracle the URL data coupled with unique identifiers that Oracle used to associate that browsing history with other data compiled into a data profile about her. On information and belief, the bk-coretag javascript code was present on a subset of websites at the time Dr. Golbeck read those articles, and that code transmitted to Oracle the URLs for the specific articles and web pages she accessed, as well as content she entered in search forms and other fields, add-to-cart actions, and other communications with websites. Oracle maintains a data profile concerning Dr. Golbeck, which Oracle provides direct or indirect access (e.g., via products or services derived from the profile) to unknown third parties. Oracle tracked Dr. Golbeck's activity on these websites, analyzed her browsing behavior and interests, and made that data, or information derived from that data (such as "segments" described at paragraphs 57, 64, and 74-76 below), via products or services derived from that profile, available to unknown third parties. On information and belief, Oracle engaged in this conduct throughout the class period. These websites visited by Dr. Golbeck include, but are not limited to:

a.   Drugs.com

b.   Health.com

c.   Healthgrades.com

d.   Mayoclinic.org

e.   Verywellhealth.com

f.   Verywellmind.com

g.   Webmd.com

16.   Oracle partnered with PlaceIQ to obtain, compile, and analyze hundreds of physical locations Dr. Golbeck had traveled to, as described above. Oracle likewise provided unknown

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   third parties with "convenient access" to Dr. Golbeck's "real world movement data."[10]   Dr.

2   Golbeck was neither aware of nor consented to this conduct. Through PlaceIQ, Oracle tracked Dr.

3   Golbeck's activity at hundreds of specific locations, including:

4   a.   retail locations;

5   b.   restaurants;

6   c.   gas stations;

7   d.   banks—including the specific type of bank and branch, thereby revealing

8   which banks Dr. Golbeck does business with.

9   17.   Oracle obtained, compiled, and analyzed information about hundreds of Dr.

10   Golbeck's credit card purchases, and then made that data, or information derived from that data,

11   available to third parties through its Data Marteeplace. On information and belief, Oracle

12   obtained, and continues to maintain in its systems, information about a vast swath of her credit

13   card purchases, including reflecting purchases for travel to specific geographic locations, specific

14   spending habits and preferences, and the "level" of spending she engages in. Dr. Golbeck was

15   neither aware of nor consented to this conduct.

16   18.   Oracle obtained, compiled, and analyzed information about Dr. Golbeck's

17   charitable donations. This information was apparently granular enough to categorize Dr. Golbeck

18   as a "religious donor."

19   19.   Oracle associated the above information with a profile through its ID Graph, as

20   described below, that contained detailed demographic information about her, as well as her name,

21   email address, physical address, and phone numbers. As such, a person in possession of any of

22   these identifiers, along with access to Oracle's dossier on her, could learn highly detailed, sensitive

23   information about her. On information and belief, unknown third parties have actually accessed

24   Dr. Golbeck's sensitive information in this manner.

25   20.   Plaintiffs are informed and believed the OARRR reflects only a small portion of the

26   information collected by Oracle on Plaintiffs since at least 2016. The OARRR does not list all of

27

28   [10] *PlaceIQ Data Now Available Through Oracle Data Cloud's BlueKai Marketplace*, PlaceIQ
     (July 13, 2016), https://www.placeiq.com/2016/07/placeiq-data-now-available-through-oracle-
     data-clouds-bluekai-marketplace/ [https://perma.cc/22T8-MVGZ].

1   the specific pieces of Plaintiffs' personal information Oracle collected, despite the provisions of

2   California Consumer Privacy Act § 1798.110 (requiring Oracle to disclose to consumers the

3   "specific pieces of personal information it has collected about that consumer."). The OARRR fails

4   to inform plaintiffs, for example, of the specific websites Oracle tracked Plaintiffs on, which can

5   thus only be learned through discovery from Oracle.

6   21.   **Defendant Oracle America, Inc.** ("Oracle" or "Defendant") is a United States

7   public corporation incorporated under the laws of the State of Delaware and is registered with the

8   State of California pursuant to California Civil Code § 1798.99.80 as a "data broker" residing at

9   500 Oracle Pkwy, Redwood City, California. On information and belief, Redwood City,

10   California is, or has been for a majority of the class period, the principle place of business for

11   Oracle and until at least December 2020, was the sole location it listed as its residence.

III.   JURISDICTION AND VENUE

13   22.   This Court has original jurisdiction over this matter pursuant to 28 U.S.C. § 1331 as

14   it arises under the laws of the United States. This Court also has subject matter jurisdiction over

15   this action pursuant to 28 U.S.C. §§ 1332 and 1367 because this is a class action in which the

16   matter or controversy exceeds the sum of $5,000,000, exclusive of interest and costs, and in which

17   some members of the proposed Classes are citizens of a state different from Defendant.

18   23.   This Court has personal jurisdiction over Defendant because Defendant conducts

19   substantial business within this District and throughout the State of California, and was

20   headquartered in Redwood City, California, for at least a substantial portion of the class period.

21   24.   Venue properly lies with this Court pursuant to 28 U.S.C. § 1391(b)(1) and (b)(2),

22   because Plaintiff Katz-Lacabe resides within this District and because Oracle maintains substantial

23   business operations in this District, and because a substantial part of the events or omissions giving

24   rise to the claims described herein occurred in this District.

IV.   CHOICE OF LAW

26   25.   California law governs the substantive legal issues in this case for the California

27   Class. The State of California has a significant interest in regulating the conduct of businesses

28   operating within its borders. California, which seeks to protect the rights and interests of

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

1   California and all residents and citizens of the United States against a company doing substantial

2   business in California, has a greater interest in the claims of Plaintiffs and Class members than any

3   other state or country and is most intimately concerned with the claims and outcome of this

4   litigation.

5   26.   Until at least December 2020, Oracle's principal place of business is, or has been

6   for the majority of the class period, Redwood City, California, where it is registered a data broker

7   under California law, where it is functioning, during the majority of the relevant time period, as

8   the "nerve center" of its business activities—the place where its high-level officers direct, control,

9   and coordinate the corporation's activities, including its marketing, software development, and

10   major policy, financial, and legal decisions.

11   27.   Oracle's privacy-invasive conduct as described herein emanated from, and was

12   conceived and executed in, California.

13   28.   Upon information and belief, the processes used to intercept, analyze, compile,

14   store and sell Plaintiffs' data are or were performed in California. At least until December 2020,

15   Oracle publicly represented that "Oracle Corporation and Oracle America, Inc., with their

16   registered address at 500 Oracle Parkway, Redwood Shores, CA, 94065, United States, are

17   responsible for the processing of your personal data."[11] The compiling of profiles on Plaintiffs

18   takes or took place in California and the provision of those profiles to third parties takes or took

19   place in California. With respect to Plaintiffs' intrusion upon seclusion and unjust enrichment

20   claims, the last acts to make Oracle liable, including the creation, maintenance, and provision to

21   third parties of these profiles, took place in California. Additionally, numerous Oracle employees

22   who were involved in effectuating and/or directing the conduct described in this Complaint reside

23   or are based in California.

24   29.   That California has a greater interest in the claims of Plaintiffs and Class members

25   than any other state or country and is most intimately concerned with the claims and outcome of

26

27   [11] *Privacy @ Oracle Data Cloud Privacy Policy*, Oracle (Last Updated Oct. 20, 2020),
     https://web.archive.org/web/20201223013611/https://www.oracle.com/legal/privacy/marketing-
28   cloud-data-cloud-privacy-policy.html#responsible [https://perma.cc/WDX7-LNL6] (under "3.
     Who is responsible for your personal data").

SECOND AMENDED CLASS ACTION COMPLAINT
                                                  CASE NO. 3:22-CV-04792-RS

1   this litigation is demonstrated by the scope of the California Consumer Privacy Act (CCPA). The

2   legislators of California recognized California's great interest in—and responsibility for—the

3   conduct of technology companies operating within its borders, and in particular California's need

4   to curtail the privacy-invasive practices of data brokers like Oracle residing or operating within

5   California. The CCPA explicitly applies to the collection or sale personal information, and only

6   exempts such conduct from its reach "if every aspect of that commercial conduct takes place

7   wholly outside of California." *See* Cal. Civ. Code § 1798.145 (Exemptions). Moreover, pursuant

8   to the CCPA, "commercial conduct takes place wholly outside of California if the business

9   collected that information while the consumer was outside of California, *no part of the sale of the*

10   *consumer's personal information occurred in California*, and no personal information collected

11   while the consumer was in California is sold." *Id.* (emphasis added). California legislators thus

12   recognize that California has a great interest in regulating the sale of its consumers' information

13   within California, even if that personal information was collected outside of California. Moreover,

14   the Ninth Circuit has recognized that under California law, if the "conduct that 'creates liability'

15   occurs in California, California law properly governs that conduct." *Oman v. Delta Air Lines, Inc.*,

16   889 F.3d 1075, 1079 (9th Cir. 2018).

17   30.   On information and belief, the sale of Class members' personal information,

18   through the Data Marketplace and the other Oracle products and services described herein, takes

19   or took place in California, regardless of which state the Class member resides in. Accordingly,

20   California has a great interest in Class members' claims against Oracle. To the extent there is any

21   factual dispute about the location of the collection, compilation, analysis, or sale of Class

22   members' personal data, that dispute must be resolved in discovery. Such discovery may

23   encompass: the location of the "nerve center" of Oracles relevant business activities, the location

24   where its high-level officers direct, control, and coordinate the corporation's relevant activities, the

25   location of the development and implementation of the software and source code that effectuates

26   Oracle's conduct described herein, and the location of the servers, electronic infrastructure, and

27   other implements that are involved in effectuating Oracle's conduct described herein, including the

28   collection, analysis, and sale of Class members' personal data.

SECOND AMENDED CLASS ACTION COMPLAINT
                                             CASE NO. 3:22-CV-04792-RS

1   31.   Application of California law with respect to Plaintiffs' and Class members' claims

2   is reasonable and fundamentally fair because California has a state interest in the claims of the

3   Plaintiffs and the Classes based upon Oracle's significant and ongoing contacts with California.

4   32.   Under California's choice of law principles, which are applicable to this action, the

5   common law of California applies to the common law claims of the California Class. Additionally,

6   given California's significant interest in regulating the conduct of businesses operating within its

7   borders, California's consumer protection laws may be applied to non-resident Plaintiffs and Class

8   members.

9   33.   The common law and statutory law of Florida applies to the Florida and FSCA

10 classes.

11 **V.   INTRADISTRICT ASSIGNMENT**

12   34.   Pursuant to Civil L.R. 3-2(c), assignment to this division is proper because a

13 substantial part of the conduct which gives rise to Plaintiffs' claims occurred in this district.

14 Defendant's conduct as described below is directed at Internet users and people throughout the

15 United States, including in Alameda County, California.

16 **VI.   STATEMENT OF FACTS**

17   35.   Oracle is one of the world's largest data brokers, in addition to its prominent public

18 facing business of database related software and data storage services, including "Oracle Cloud"

19 that developers may use to build and run internet sites and mobile applications.[12] Oracle reaps

20 great financial benefit from its conduct described herein; while the revenue attributable to its data

21 broker businesses is not publicly disclosed, Oracle's market capitalization exceeds $227 billion.

22   36.   As a data broker, Oracle facilitates the buying and selling of digital data, including

23 personal information, among private commercial and governmental entities. Oracle operates a

24 data management platform called the BlueKai Data Management Platform (now also known as

25 "Oracle Data Management Platform" or "Oracle DMP"[13]), which includes two key features: the

26

27 [12] *Oracle Products, Solutions, and Services*, Oracle, https://www.oracle.com/products/
    [https://perma.cc/96FG-AYQC].

28 [13] *See Integrating Oracle Eloqua and Oracle DMP*, Oracle (May 5, 2023),

SECOND AMENDED CLASS ACTION COMPLAINT
                                                    CASE NO. 3:22-CV-04792-RS

1   Oracle Data Marketplace and the Oracle ID Graph. The Oracle Data Marketplace is one of the

2   world's largest, if not the largest, commercial data exchange, with a broad impact upon the lives of

3   most Americans and many millions of people worldwide.[14]

4   37.   The Oracle ID Graph is a service product designed to provide "identity resolution,"

5   the process of "matching individual customer identities . . . and combining them into a single

6   consistent and accurate customer profile."[15] Oracle's ID Graph "synchronizes" the vast amounts

7   of personal data Oracle has amassed; that is, it matches personal data that can be determined to

8   share a common origin with other personal data. This synchronizing allows Oracle to identify

9   individuals and aggregate their many identifiers, which in turn facilitates further synchronizing of

10   personal data with a high degree of confidence. As Oracle, in velveteen marketing language,

11   describes it:

12   The Oracle ID Graph helps marketers connect identities across disparate marketing
             channels and devices to one customer. Powered by the Oracle Marketing Cloud
13   and Oracle Data Cloud, the Oracle ID Graph seamlessly pulls together the many
             IDs across marketing channels and devices that comprise a given person, enabling
14   marketers to tie their interactions to an actionable customer profile. This ID
             enables the marketer to orchestrate a relevant, personalized experience for each
15   individual across marketing channels and device types.[16]

16   38.   Oracle and other data brokers act as central nodes in the "adtech" network, where

17   massive volumes of personal information on the world's population is aggregated and used to

18   identify and profile individuals for "targeted advertising" or other commercial and political

19   purposes.

20   39.   Oracle tracks the lives of the general public in a manner that is opaque, if not

21   invisible, to the people it follows, as they have no direct relationship with Oracle. Oracle is

22   registered as a "data broker" in California (and in other States), which is defined as "a business

23   _____

     https://docs.oracle.com/en/cloud/saas/marketing/eloqua
24   user/pdf/OracleEloqua_BlueKai_AdminGuide.pdf [https://perma.cc/H5FA-BPQW] ("Important:
     Oracle BlueKai is now known as Oracle DMP").

25   [14] Giridhari Venkatadri, Piotr Sapiezynski, et al., *Auditing Offline Data Brokers via Facebook's
     Advertising Platform*, The World Wide Web Conference (May 13-17, 2019), https://lig-
26   membres.imag.fr/gogao/papers/databrokers-measurement_finalCameraReady.pdf
     [https://perma.cc/H7XW-PWE2].
27   [15] *What Is a Customer Data Platform*, Oracle, https://www.oracle.com/bh/cx/customer-data-
     platform/what-is-cdp/ [https://perma.cc/FBW7-X8DP].
28   [16] *ID Management,* Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-
     center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].

                                                                  SECOND AMENDED CLASS ACTION COMPLAINT
                                    - 13 -   CASE NO. 3:22-CV-04792-RS

1   that knowingly collects and sells to third parties the personal information of a consumer with

2   whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80. As such,

3   Oracle does not even maintain a pretense of having directly obtained the consent of the subjects of

4   its surveillance—i.e., the proposed Classes herein—who have no legal or practical ability to

5   consent to Oracle's conduct.

6   40.   Oracle's business model has long roots in the surveillance of ordinary citizens.

7   Oracle takes its name from a CIA project codename. In 1977, Oracle's founder, Larry Ellison,

8   was hired by the CIA to build a database; the CIA was Oracle's first customer. As of 2020, Oracle

9   had contracts with all five branches of the military, and recent or pending contracts with the CIA,

10 as well as substantial relationships with local law enforcement across the country. Surveillance is

11 central to Oracle's history and development, and to its current business and marketing plan.

    A.   **Oracle Employs Multiple Methods for the Collection of Personal Data from Unwitting Internet Users.**

12

13

14   41.   Operation of Oracle's ID Graph depends upon the accumulation of vast amounts of

15 personal data concerning as many people as possible. Oracle utilizes multiple means to collect and

16 aggregate the personal data of people worldwide, including the primary methods alleged in this

17 subsection.

18   42.   Oracle collects many types of personal information from Internet users including

19 concrete identifiers such as names, home and work addresses, e-mail addresses, and telephone

20 numbers. Oracle also amasses data about peoples' behavior, including the sites they visit online,

21 their digital and offline purchases, where they shop, and how they pay for their purchases. Oracle

22 gathers this personal information from a suite of its own Internet technologies, including cookies,

23 tracking pixels, device identification, cross-device tracking, as well as from its acquisition of data

24 from other parties. Oracle then processes, analyzes, and monetizes this data, as described below.

25   43.   Cookies. Oracle deploys its own proprietary "cookies" which are pieces of

26 software code sent by Oracle that are stored on Internet users' web browsers and collect

27 information regarding Internet use. Oracle's cookies are frequently labeled "BlueKai," named

28 after a start-up Oracle acquired in February 2014. Oracle's BlueKai cookies track online and

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   mobile app activity, obtaining data in real time and transmitting it back to Oracle's servers. When

2   an Internet user visits a webpage or uses a mobile application, Oracle employs its BlueKai cookies

3   to gather and transmit to itself information including the unique user ID, IP address, session time,

4   number of sessions or visits, the URL or websites an Internet user has visited (*e.g.*, Referrer and

5   Origin headers), hyperlinks clicked, and documents downloaded.[17] Oracle is able, with the use of

6   algorithmic data processing, to use the data it gathers from BlueKai cookies (and, as explained

7   below, which may also be associated with additional data from other sources) to infer a wide range

8   of behavioral traits and information that it attributes to individual Internet users through persistent

9   identifiers or other personal information of the Internet users—including their consumer

10   preferences, income levels, and their politics.

11   44.   JavaScript. Oracle utilizes a proprietary software device, referred to as "bk-

12   coretag.js" JavaScript code, to "extract," or intercept, "user attributes," which include the contents

13   of users' communications with websites, and secretly sends them to Oracle while the users are in

14   the process of communicating with those websites. Oracle's technical documentation explains that

15   bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views,

16   purchase intent, [and] add-to-cart actions"[18] and other communications that users have with

17   websites and simultaneously copies and sends those communications to Oracle.

18   45.   Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices

19   when they browse a website that contains certain Oracle code. When an individual Internet user

20   visits a webpage, his or her browser sends a message called a "GET request" to the webpage's

21   server. The GET request tells the website what information is being requested and also instructs

22   the website's server to send the information back to the user. The bk-coretag.js JavaScript code

23   then communicates with Oracle's servers and source code by sending separate "GET" requests to

24

25   ───────────────

26   [17] Martin Degeling & Jan Nierhoff, *Tracking and Tricking a Profiler Automated Measuring and Influencing of Bluekai's Interest Profiling*, Workshop on Privacy in the Electronic Society (Oct. 15, 2018), https://dl.acm.org/doi/pdf/10.1145/3267323.3268955 [https://perma.cc/7UVK-ALU9].

27   [18] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-

28   center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

1   Oracle that contain copies of contents in the initial "GET" request being sent by the user's browser

2   to the website they are visiting.

3   46.   Oracle uses the bk-coretag.js JavaScript code to intercept the contents of Internet

4   users' communications with websites as follows:

5   a.   When a user opens an Internet webpage that contains certain code, a

6   request is sent by the user's browser to Oracle's servers to fetch the bk-coretag.js JavaScript file.

7   b.   The bkcoretag.js code then triggers a series of additional network "GET"

8   requests.

9   c.   As part of these "GET" requests, the bk-coretag.js code intercepts the

10   contents of the user's communications with the browser and simultaneously copies those contents

11   and sends them to Oracle.

12   47.   Through this practice, Oracle is able to intercept substantive communications

13   between internet users and websites, including, inter alia: [19]

14   a.   the URLs being browsed by the Internet user as well as the referrer URL;

15   b.   webpage title;

16   c.   webpage keywords;

17   d.   the exact date and time of the website visit;

18   e.   the IP address of the user's computer;

19   f.   product page visits;

20   g.   "purchase intent"[20] signals;

21   h.   "add-to-cart actions"; and

22   i.   data entered by the user into forms on the website.

23

24

[19] *Data Ingest*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-
25   center/IntegratingBlueKaiPlatform/data_ingest.html [https://perma.cc/99JS-5Z64].

26   [20] Oracle's technical documentation does not appear to define the term "purchase intent,"
     however an Oracle document describes "Interest and intent signals" as including "search, page
27   views, and price comparison." *See Activation Playbook*, Oracle (2020),
     https://www.oracle.com/za/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf
28   [https://perma.cc/TYS5-NKX4].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                                              CASE NO. 3:22-CV-04792-RS

1   48.   The bk-coretag.js code also sends to Oracle the Internet user's login status and

2   "hashes" of the user's email address and phone number.[21] Oracle attributes the communications to

3   specific individuals using identifiers, such as email address, phone number, or account ID, and

4   then uses this data to enrich its user profiles and ID Graph and classify users into categories for

5   targeting.[22]

6   49.   Oracle's technical documentation also explains that bk-coretag.js engages in

7   "synchronous" communication interception, i.e., interception while the communication is in

8   transit, which "[s]ends data to the Oracle Data Cloud platform as quickly as possible . . . while the

9   web browser loads."

10   50.   Oracle's bk-coretag.js JavaScript code has been recognized by security researchers

11 as a tracking mechanism for surreptitiously monitoring and intercepting user's internet

12 communications and activity. It has been described as "click interception script" that intercepts

13 clicks by users on webpages,[23] and as an online activity "tracker" that can "learn a sizable chunk

14 of the browsing history of a given user, and likely without their knowledge."[24]

15   51.   Tracking Pixels. Another tool utilized in Oracle's digital tracking efforts are

16 "tracking pixels." Tracking pixels are pieces of code that are embedded into webpages and mobile

17 applications built with Oracle's technology, such as Oracle Cloud. Oracle tracking pixels are

18 essentially invisible to Internet users because they are hidden within the code of a webpage and

19 activate (or "fire") whenever the page is opened, regardless of and prior to any pretense of consent

20

21 [21] According to Oracle, "Hashing is a form of encryption used for swapping data between
    integrated data management systems." *See Hashing Identifier*, Oracle,
    https://docs.oracle.com/en/cloud/saas/marketing/eloqua-user/Help/General/HashingIdentifier.htm

22 [https://perma.cc/C59Q-X4PC].

23 [22] *Oracle Data Cloud Core Tag Implementation*, Oracle,
    https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-
    center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html

24 [https://perma.cc/8XVU-8Z2F].

25 [23] Mingxue Zhang, Wei Meng, et al., *All Your Clicks Belong to Me: Investigating Click
    Interception on the Web*, Proceedings of the 28th USENIX Security Symposium (Aug. 14-16,

26 2019), https://www.usenix.org/system/files/sec19fall_zhang_prepub.pdf [https://perma.cc/8A9V-
    URWL].

27 [24] *See* Zhonhao Yu, Sam Macbeth, et al., *Tracking the Trackers*, World Wide Web Conference
    (April 11-15, 2016), http://josepmpujol.net/public/papers/pujolTrackingTheTrackers.pdf

28 [https://perma.cc/WT3W-TW5U].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                       CASE NO. 3:22-CV-04792-RS

being sought. Unlike cookies, tracking pixels cannot be disabled. When a user visits a site with an Oracle pixel, the company receives, at minimum, the full URL, time zone, screen resolution, browser window resolution, and title of the webpage.[25] Consequently, if a person visits, for example, a specific product page on a retailer's website, Oracle instantly knows about it and, as with cookies, adds the information to the person's profile in Oracle's database. Nor are pixels confined to websites: Oracle pixels are in marketing emails from numerous companies—when the email is opened, the pixels identify the specific reader and the underlying marketing campaign.[26]

52.   This data collection is not dependent upon any relationship that an Internet user may or may not have with Oracle. In fact, Oracle primarily collects data through its BlueKai cookies and pixels from persons having no privity whatsoever with Oracle. Even privacy-conscious users who endeavor to understand the origins of Oracle cookies may not know Oracle is amassing data about them because Oracle's cookies and pixels do not bear the company's name.

53.   Oracle's cookies and tracking pixels are pervasive throughout the Internet. [27] Oracle has agreements with numerous high-traffic websites like the New York Times, ESPN, and Amazon to place cookies and/or pixels on their websites.[28] By blanketing popular websites with these tracking tools, Oracle reaches a substantial percentage of Internet users—Oracle cookies are found on over 20 percent of the top 10,000 websites[29] and more than 48 thousand websites.[30]

---

[25] *Device Fingerprints and Custom Sign In Pages*, Oracle, https://docs.oracle.com/en/cloud/paas/identity-cloud/uaids/use-device-fingerprints.html#GUID-17B61B5F-7937-4830-8368-075EE2001BDF [https://perma.cc/56VS-XQFU].

[26] *Activating Eloqua Email Marketing Data*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/ManagingTaxonomy/ingest_partners/eloqua_email_data_activation.html [https://perma.cc/A8ZZ-HLF7].

[27] *Host Search Results: bluekai.com*, Cookiepedia, https://cookiepedia.co.uk/host/bluekai.com [https://perma.cc/RHA9-KTRB].

[28] Wolfie Christl (@wolfiechristl), Twitter (Mar. 23, 2018, 12:55 PM), https://twitter.com/WolfieChristl/status/977272603038633985?s=20.

[29] Additionally, a Dutch action against Oracle alleges its cookies are found on at least 28 of 100 of the most popular websites in the Netherlands. *Writ (For The Main Action)*, The Privacy Collective (Aug. 26, 2020), https://theprivacycollective.nl/wp-content/uploads/2020/11/Writ-of-Summons-English-translation-26-August-2020.pdf [https://perma.cc/4AKV-XNRY] (¶ 427).

[30] *Oracle BlueKai*, NerdyData, https://www.nerdydata.com/reports/oracle-bluekai/e99ff880-6d16-45d1-94c7-6cce7ae1571d [https://perma.cc/64ME-U27H].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

54. <u>Device Identification.</u> Oracle tracks users by harvesting and exfiltrating user "device identifiers." Oracle is able to track Class members' online activities by collecting identifiers tied to their devices. These identifiers include IMEI (International Mobile Equipment Identity), MAC address (Media Access Control address), and Mobile Advertising ID (MAID) such as Advertising Identifier (IDFA) on iOS and Advertising ID (ADID) on Android devices.[31]

55. <u>Cross-device Tracking.</u> Oracle monitors Class members' activities across their devices through cross-device tracking. When Class members shop online at home on their iPad, read the news on their iPhone during their commute, and visit sites on their laptop at work, Oracle monitors and collects their movements.[32] Oracle also tracks activity through television and touts its ability to monitor viewing habits and measure the effectiveness of advertising in video games.[33] Oracle thereby allows its customers to target Plaintiffs and Class members *across their devices* with the flip of a switch, as this graphic from Oracle illustrates:[34]

---

[31] *Fingerprinting Types*, Oracle,
https://docs.oracle.com/cd/E52734_01/oaam/AAMAD/finger.htm#AAMAD9008
[https://perma.cc/252P-6BN9].
[32] *ID Management,* Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].
[33] Glenn Bean, *How Moat Reach Captures Cross-Platform Reach and Frequency-and Why it's Better Than What You Have Today*, Oracle Advertising Blog (Jun. 3, 2020),
https://blogs.oracle.com/advertising/post/how-moat-reach-captures-cross-platform-reach-and-frequencyand-why-its-better-than-what-you-have-today [https://perma.cc/YMG6-DT8N]; *TV & Digital Campaign Measurement*, Oracle, https://www.oracle.com/cx/advertising/measure-campaign-effectiveness/cross-platform-measurement/ [https://perma.cc/W55S-ZUC9] ; *Industry first: In-game measurement for 3D advertisements*, Oracle,
https://www.oracle.com/cx/advertising/data-enrichment-measurement/#ingame-measurement
[https://perma.cc/9DEK-9FJV].
[34] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

Cross Device Settings ×

Cross device extension, powered by the Oracle ID Graph™, connects people across all their devices and is currently only available in the United States and **these countries.**

🔵 Cross Device

People Reach: 108M - 128M

Current Reach		Cross Device*		Final Reach	
Desktop Cookies	219M	Desktop Cookies	+136M - 252M	Desktop Cookies	355M - 471M
Mobile Cookies	248M	Mobile Cookies	+143M - 266M	Mobile Cookies	392M - 515M
Android AdIDs	397M	Android AdIDs	+315M - 586M	Android AdIDs	712M - 983M
Apple IDFAs	296M	Apple IDFAs	+225M - 419M	Apple IDFAs	522M - 715M

*Cross Device counts are only available for Device ID's within the United States.

[Cancel] [Save Settings]

56.   AddThis. AddThis was a widget, or a piece of code that web developers incorporate into a website that provided a graphical user interface that displays information and provides a means for a user to interact with the website, which Oracle acquired in 2016. With an AddThis enabled website, Internet users could bookmark or post the webpage to their various social media platforms including Facebook, Pinterest, and Twitter. These plugins, which are free, were ubiquitous: As of 2022, AddThis was used on 15 million websites and purported to offer "insight into the interests and behaviors of over 1.9 billion web visitors," and its "vast global footprint reaches 96% of the U.S. web."[35] Whenever an Internet user visited a website with an AddThis plugin, the user was subjected to cookies and pixels, without any notice or practical ability for detection, and as a result, Internet users were unaware that Oracle was tracking and recording their online activity for purposes of identifying the Internet users and their activities to Oracle and its customers. Recent forensic analysis has confirmed that AddThis was ubiquitous and tracked data from sites related to sensitive health and personal safety information: AddThis

_____

[35] *About Us*, AddThis (2022), archived at https://perma.cc/JK9N-3W3Z.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

trackers were found on more than 4,000 popular websites, as well as four states' coronavirus

information pages.[36] AddThis trackers were also found on websites with resources for

undocumented immigrants, domestic violence survivors, and the LGBTQ community.[37] Human

Rights Watch, concerned about Oracle's collection of data from children, has noted that:

> . . . AddThis does much more than encourage social media traffic. Whether or not
> a person clicks on the "share" button, AddThis instantly loads dozens of cookies
> and tracking pixels on website visitors' browsers, like nesting dolls, each
> collecting and sending user data to Oracle and to dozens of other AdTech
> companies to profile and target a person or a child with behavioral advertising that
> follows them across the internet.[38]

Oracle recently announced that it had "terminate[d] all AddThis services effective as of May 31,

2023"—only days after the First Amended Complaint in this action was filed on May 22, 2023,

and over eight months after the original Complaint in this action was filed on August 19, 2022.[39]

Plaintiffs' investigation into the nature and extent of Oracle's "terminat[ion]" of this conduct is

ongoing.

57.   Datalogix. In 2014, Oracle acquired Datalogix, an information broker specializing

in profiling people based on their purchases at brick-and-mortar retailers, primarily by purchasing

and aggregating data from retailers' loyalty programs. In 2019, an Oracle executive explained the

colossal scale of this data as including, "115 million U.S. households, 10 billion SKU-level

transactions, over 1,500 leading brands, and $5 trillion in consumer spending data."[40] Datalogix's

coverage was found by academic researchers to be up to 76.2% in the U.S. and 43.6% in the

U.K.[41] Datalogix data is now referred to as "Oracle Datalogix (DLX) data" and is described by

---

[36] Aaron Sankin & Surya Mattu, *The High Privacy Cost of a "Free" Website*, The Markup (Sept. 22, 2020, 6:00 AM ET), https://themarkup.org/blacklight/2020/09/22/blacklight-tracking-advertisers-digital-privacy-sensitive-websites [https://perma.cc/X66F-79D6].

[37] *Id.*

[38] *"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic*, Human Rights Watch (May 25, 2022), https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments [https://perma.cc/3R2D-46PM].

[39] *See Notice of Termination of AddThis Services*, AddThis (November 17, 2023), https://www.addthis.com/ [https://perma.cc/3PT9-2AKF].

[40] *Audience Targeting with Oracle: Q&A with Oracle Data Cloud's Dan Loewenberg*, Spot X (Mar. 21, 2019), https://www.spotx.tv/resources/blog/product-pulse/audience-targeting-with-oracle-qa-with-oracle-data-clouds-dan-loewenberg [https://perma.cc/6T3N-TY2Z].

[41] Giridhari Venkatadri, Piotr Sapiezynski, et al., *Auditing Offline Data Brokers via Facebook's*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   Oracle as "the premier solution when looking for offline purchase- and activity-based

2   audiences."[42] Among Oracle's current product offerings is the "Datalogix Profile Analysis" which

3   provides advertisers with "Demographic Segments," "Lifestyle Segments, Retail Behavioral

4   Segments, and Purchase Behavioral Segments" on Internet users.[43]

5   58.   Data From Third Parties. Oracle enhances the personal information that it collects

6   from Internet users with personal information collected and sold by other third-party data brokers.

7   The personal information Oracle amasses through its tracking technologies together with the

8   personal information collected by third parties includes billions of data points on more than 300

9   million users, or over 80% of the entire U.S. population.[44]

10   59.   When an Internet user uses a website employing the Oracle tracking technologies

11   described above, Oracle can track and store behavioral activity and personal information,

12   including, but not limited to, home location, age, income, education, family status, hobbies,

13   weight, and what the user bought at a brick-and-mortar business yesterday afternoon. Internet

14   users are not made aware of, and therefore cannot consent to, use of their information to facilitate

15   Oracle's personal identification enterprise, the "Oracle ID Graph."

16   **B.   Oracle Uses The Personal Data of Internet Users To Fuel Its Personal
              Identification and Profiling Product "Oracle ID Graph."**
17

18   60.   Oracle has developed the "Oracle ID Graph" using the vast stores of personal data

19   it has accumulated. Oracle designed the Oracle ID Graph to have the capability of identifying

20   Internet users and compiling personal data associated with them, including so-called "anonymous"

21

22   _____

23   *Advertising Platform*, The World Wide Web Conference (May 13-17, 2019), https://lig-
     membres.imag.fr/gogao/papers/databrokers-measurement_finalCameraReady.pdf
     [https://perma.cc/H7XW-PWE2].

24   [42] *Datalogix by Oracle Data Cloud*, Twitter, https://partners.twitter.com/en/partners/datalogix-by-
     oracle-data-cloud [https://perma.cc/N855-D5VV].

25   [43] *Using the Datalogix Profile Analysis Dashboard*, Oracle,
     https://docs.oracle.com/en/cloud/saas/marketing/cx-audience-
26   user/AudienceInsight_DLXDashboard.htm#Using [https://perma.cc/G4DM-BWR8].

27   [44] *Oracle Data Marketplace*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-
     help-center/AudienceDataMarketplace/AudienceDataMarketplace.html [https://perma.cc/27S8-
28   GX7H].

SECOND AMENDED CLASS ACTION COMPLAINT
                                        CASE NO. 3:22-CV-04792-RS

1   data which Oracle re-identifies to specific individuals. Oracle makes the Oracle ID Graph

2   available for sale to private and governmental purchasers on its Data Marketplace.

3   61.   In April 2015, Oracle unveiled Oracle ID Graph as a new feature of the BlueKai

4   data management platform.[45] The introduction of Oracle ID Graph permitted the compiling of an

5   Internet user's various disaggregated identifiers. Previously, because browsers, devices, and

6   mobile applications each use a different identifier, identification of users was typically limited to a

7   single device. The Oracle ID Graph processes available personal data, digital identifiers (such as

8   "browser cookies, mobile advertising IDs, IP addresses, and console IDs"), and concrete

9   identifiers (such as "hashed first names, last names, postal addresses, email addresses, and

10   telephone numbers") to identify and establish "a single, universal view of identity" for each user.[46]

11   In addition to connecting and associating multiple browser and device identifiers, the Oracle ID

12   Graph combines these identifiers with demographic, behavioral, and biographic data, ranging from

13   marital status to hair type to college major to household location, to enhance the profiles of

14   individuals within its ID Graph.[47]

15   62.   Oracle has described its ID Graph as the "backbone technology [that] powers all

16   Oracle Data Cloud solutions," allowing Oracle's customers to track individual people "seamlessly

17   across devices (desktop and mobile) and channels (offline and online) via more than 200 media

18   and marketing platforms, including the largest and fasted-growing consumer platforms."[48]

19

20   [45] *Oracle Energizes Its Marketing Cloud With New Features*, Forbes (Apr. 7, 2015), https://www.forbes.com/sites/greatspeculations/2015/04/07/oracle-energizes-its-marketing-cloud-with-new-features/?sh=1db7452b7852 [https://perma.cc/WT53-CYEH].

21   [46] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018), https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf

22   [https://perma.cc/WW3A-HVBA].

23   [47] *Activation Playbook*, Oracle (2020), https://www.oracle.com/ca-fr/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].

24   [48] *Powered by Oracle ID Graph*, Oracle, https://web.archive.org/web/20180826201234/https://www.oracle.com/applications/customer-

25   experience/data-cloud/solutions/id-graph.html [https://perma.cc/SG2R-VQKS]. Oracle further describes the ID Graph as follows: "The Oracle ID Graph is not a product but it is a foundational

26   capability or technology that power[s] the Oracle [Bluekai Data Management Platform]. All linkages in Oracle ID Graph are continuously validated and scored, which changes dynamically

27   based on a proprietary algorithm to the input . . . . Oracle ingests massive amounts of IDs across cookies, login, HH, email, and mobile ad IDs on a weekly or sometimes daily basis from ID data

28   partners." *See Unite Disparate Data to Make It Actionable*, Oracle,

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

63.   The Oracle ID Graph is an example of the practice known in the adtech industry as "identity resolution." As Oracle explains, the Oracle ID Graph lets its customers "connect identities across disparate marketing channels and devices to one customer" by "seamlessly pull[ing] together the many IDs across marketing channels and devices that comprise a given person, enabling marketers to tie their interactions to an actionable customer profile."[49] The following illustration from Oracle describes this process:[50]
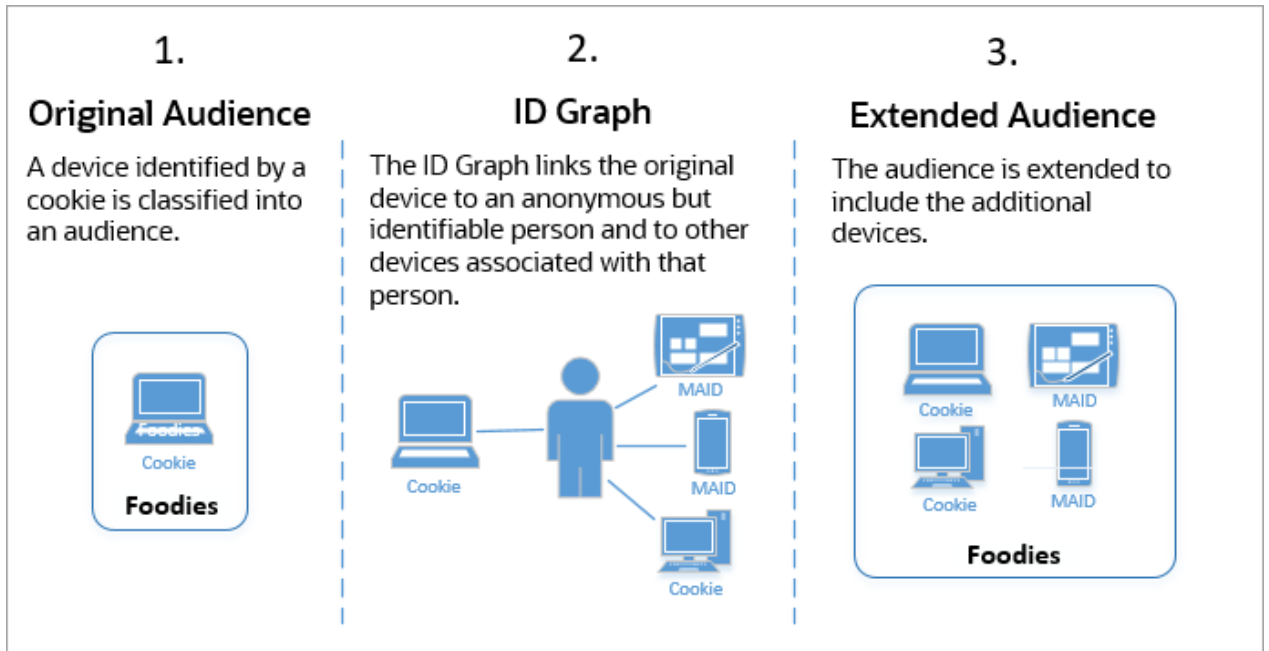
64.   Oracle's identity resolution process consists generally of three steps:

a.   ***First,*** Oracle filters the data it collects, from BlueKai cookies, pixels and other sources, into millions of individual profiles on Class members. Data from, *inter alia*, "$90B in transactions tied to real people every week," "digital ID graphing on 115MM+ households," and "a global network of 15MM websites" is validated, compared, and combined into "a single, universal view of identity." The ensuing profiles are exceedingly detailed. They include digital

---

https://web.archive.org/web/20210119032758/https://www.oracle.com/data-cloud/products/data-management-platform/id-graph.html [https://perma.cc/Y5A5-MXL3].

[49] *ID Management,* Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/id_management.html [https://perma.cc/LCW9-9PCH].

[50] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF] (the reference to "MAID" refers to a "mobile advertising ID").

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   identifiers like "browser cookies, mobile advertising IDs, IP addresses, and console IDs," and

2   hard data such as "hashed first names, last names, postal addresses, email addresses, and

3   telephone numbers."[51] This is in addition to the details that Oracle layers onto these core

4   identifiers, including offline and geolocation data. As Oracle describes it, the "promise" of the ID

5   Graph "is to connect identifiers to the consumer online and offline. Offline data ties the identity

6   graph to *real people living at a real address*, not just a mixture of device IDs and cookies.

7   Identity graphs built from offline *and* online signals are better connected and validated."[52]

8   b.   *Second***,** Oracle applies analytics to extract yet more information from the

9   profiles it has created. An Oracle profile has hundreds or thousands of data points; Oracle then

10   infers from this raw data that, for example, a person isn't sleeping well, or is experiencing

11   headaches or sore throats, or is looking to lose weight, and thousands of other invasive and highly

12   personalized inferences.[53]

13   c.   This process provides Oracle with a virtual panopticon: Oracle purports to

14   have vision on virtually everything ascertainable in electronic form about Class members, from

15   where they live, to the media they consume, to the things they buy, to the views they hold.[54] The

16   following examples illustrate the extraordinary breadth of the data that Oracle's customers can

17   access via Oracle ID Graph:

18   *Address:* Oracle has an address for over 110 million households, and lets clients
          target households within a radius of a given location.[55]

19
          Life Events: Oracle can target based on major life events, including marriage,
20   childbirth, job changes, and graduation.[56]

21

22

23   [51] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018),
     https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf
24   [https://perma.cc/WW3A-HVBA].
     [52] *Id.*(emphasis added).
25   [53] *Oracle Data Cloud Health and Wellness Segments (US only)*, Oracle (Last Updated Oct. 14,
     2020), https://www.oracle.com/a/ocom/docs/corporate/health-and-wellness-segments.pdf
26   [https://perma.cc/37T2-FG4Q].
     [54] *Activation Playbook*, Oracle (2020), https://www.oracle.com/za/a/ocom/docs/cx-activation-
27   vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].
     [55] *Id.*
28   [56] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

Education: Oracle segments by degree obtained, type of school (*e.g.* public, private, community college, online), and even major.[57]

Purchase History: Oracle can filter for specific purchases—made both in brick-and-mortar establishments and online—such as "Alcohol Beverage purchase based modeled audiences," including micro-targeting categories tracking people's alcohol use habits, such as "Malt Beverage Buyers" or "Wine or Liquor Store Top Spenders."[58]

Health & Wellness: Oracle segments people based on intimate information, including a person's views on their weight, hair type, sleep habits, and type of insurance.[59] Other categories appear to be proxies for medical information that Oracle purports not to share, like "Emergency Medicine," "Imaging & Radiology," "Nuclear Medicine," "Respiratory Therapy," "Aging & Geriatrics" "Pain Relief," and "Allergy & Immunology."[60]

d.   **Third,** Oracle matches the data provided by its customers to the existing profiles of individuals it has developed. Using "Oracle OnRamp," the company "ingests [customers'] PII [personally identifiable information] and matches it to 115MM U.S. households, first names, last names, and telephone numbers."[61] Oracle clients can then target (or exclude) Class members based on attributes in Oracle profiles, and purchase yet more customer information from the Oracle Data Marketplace.

e.   The matching process also helps Oracle's clients to knit together aspects of their own data sources. For instance, tying previously siloed online and offline information to an Oracle profile might reveal the user who last week visited a business's website is the same person who yesterday made purchases at a particular brick-and-mortar store belonging to that same business.[62] The image below illustrates the process.[63]

---

[57] *The Audience Playbook*, Oracle, at 11 (Aug. 2016), http://online.pubhtml5.com/mdhz/hgpp/#p=11 [https://perma.cc/L6WS-ND8L].

[58] *Alcohol and Beverage Digital Audiences and Contextual Segments*, Oracle, https://www.oracle.com/middleeast/a/ocom/docs/beverage-digital-audiences-contextual-segments.pdf [https://perma.cc/YEL7-DKG6].

[59] *Oracle Data Cloud Health and Wellness segments (US only)*, Oracle, (Last updated Oct. 14, 2020) https://www.oracle.com/a/ocom/docs/corporate/health-and-wellness-segments.pdf [https://perma.cc/37T2-FG4Q].

[60] *Id.*

[61] *12 Must-Ask Questions to Separate Fact From Fiction*, Oracle (2018), https://www.oracle.com/a/ocom/docs/idg-12-must-ask-questions-for-identity-vendors.pdf [https://perma.cc/WW3A-HVBA].

[62] *Id.*

[63] *Offline Match Integration*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/offline_match.html [https://perma.cc/2QXQ-TNY4]. Oracle offers clients other ways to ingest customer data, but regardless of means the

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1
2
3
4
5
6
7
8

9
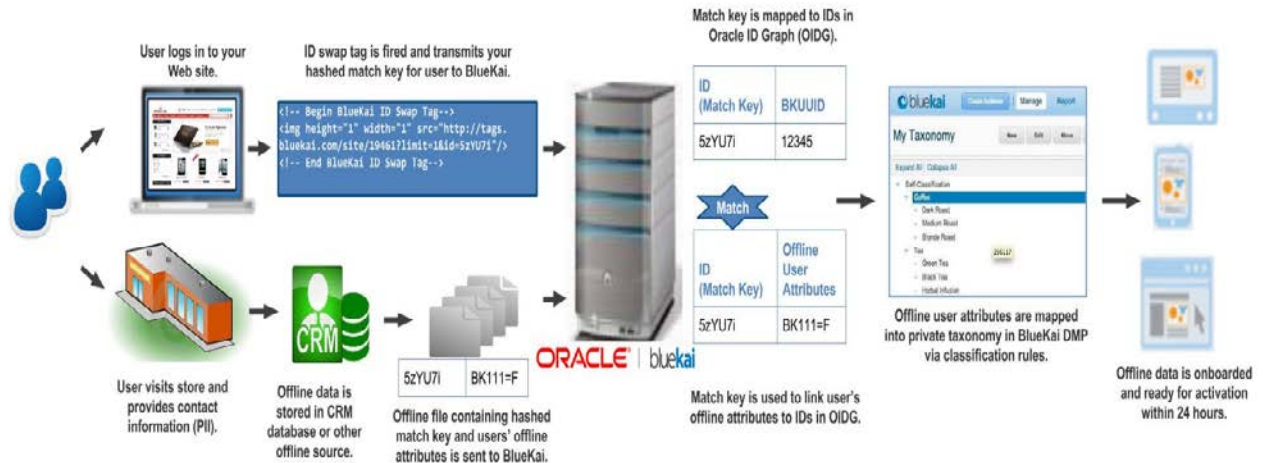
10   65.   Oracle ID Graph relies on "ID swapping" to "synchronize" or match unique user

11   IDs (UUIDs) of Class members between Oracle Data Cloud Platform and its clients. Oracle ID

12   Graph employs a variety of deterministic and probabilistic matching techniques to this end.[64] The

13   combination of deterministic and probabilistic techniques to construct the Oracle ID Graph is one

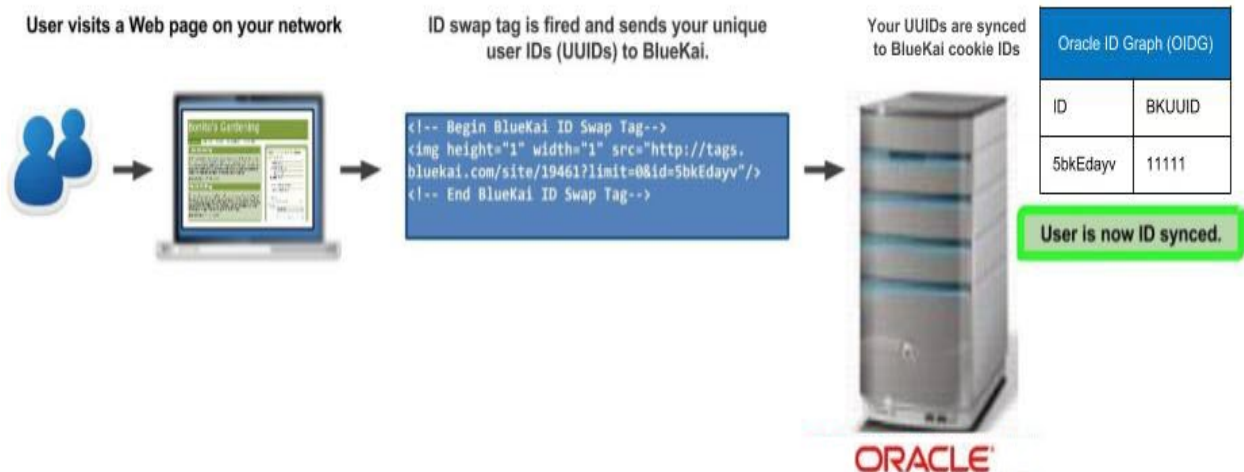14   of its distinguishing features.[65] This process includes the following technical features:

15
16
17
18
19
20
21
22
23

24   result—uploading customer data to the Oracle Data Cloud—is the same. The other options are
     summarized at *Data Ingest*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-
25   help-center/IntegratingBlueKaiPlatform/data_ingest.html [https://perma.cc/S2FZ-EYLD].

     [64] *Deterministic and Probabilistic Data Matching*, Oracle (2010),
26   https://docs.oracle.com/cd/E19182-01/821-0919/ref_sme-deter-probl_c/index.html
     [https://perma.cc/NCL3-QYHD].

27   [65] Audrey Rusch, *When it Comes to Identity, Probabilistic or Deterministic is Not the Question*,
     Oracle, (Aug. 19, 2019), https://blogs.oracle.com/advertising/post/when-it-comes-to-identity-
28   probabilistic-or-deterministic-is-not-the-question [https://perma.cc/5EQE-REXV].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                        CASE NO. 3:22-CV-04792-RS

a.   Oracle employs a "tag" to exfiltrate Class members' personally identifiable information such as email addresses, phone numbers, physical addresses, account numbers, Twitter handles, and other information to Oracle for a deterministic match.[66] Even if the personally identifiable information is hashed before being exfiltrated to Oracle, it can be easily reversed and thus does not provide any privacy as compared to no hashing.[67]

b.   Oracle employs "cookie sync" technology[68] to link cookie-based identifiers of Class members between Oracle Data Cloud Platform and its clients for a deterministic match.[69] Cookie syncing is used by Oracle to circumvent the security feature of web browsers called "Same Origin Policy" that aims to prevent data sharing between different parties.[70] Cookie syncing also helps Oracle circumvent privacy features in web browsers, such as Safari, that block third-party cookies.[71]

---

[66] *ID Swapping*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/id_swap.html [https://perma.cc/54R4-JKAM].

[67] Gunes Acar, *Four Cents to Deanonymize: Companies Reverse Hashed Email Addresses*, Freedom to Tinker (Apr. 9, 2018) https://freedom-to-tinker.com/2018/04/09/four-cents-to-deanonymize-companies-reverse-hashed-email-addresses/ [https://perma.cc/4J9T-2Q6G].

[68] *Oracle BlueKai Glossary*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Glossary/OracleBlueKaiGlossary.htm [https://perma.cc/NBK7-N2H7].

[69] Zach Rodgers, *In A Year Of Data Disruption, Oracle Places Its Bets*, Ad Exchanger (Sept. 9, 2020) https://www.adexchanger.com/adexchanger-talks/in-a-year-of-data-disruption-oracle-places-its-bets/ [https://perma.cc/VV9E-TCXR].

[70] Panagiotis Papadopoulos, Nicolas Kourtellis, et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, The World Wide Web Conference (May 13-17, 2019), https://arxiv.org/pdf/1805.10505.pdf [https://perma.cc/F4UJ-CHZ8].

[71] Quan Chen, Panagiotis Ilia, et al., *Cookie Swap Party: Abusing First-Party Cookies for Web*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

c.   For Class members using mobile apps where cookies may not be present, Oracle uses Mobile advertising IDs (MAIDs) that are derived from mobile apps (e.g., Identifier for Advertisers [IDFA] on iOS[72] and Google Advertising ID [AAID] on Android[73]) for a deterministic match.[74] MAIDs are linked by data brokers to "a person's full name, physical address, and other personal identifiable information (PII)".[75]
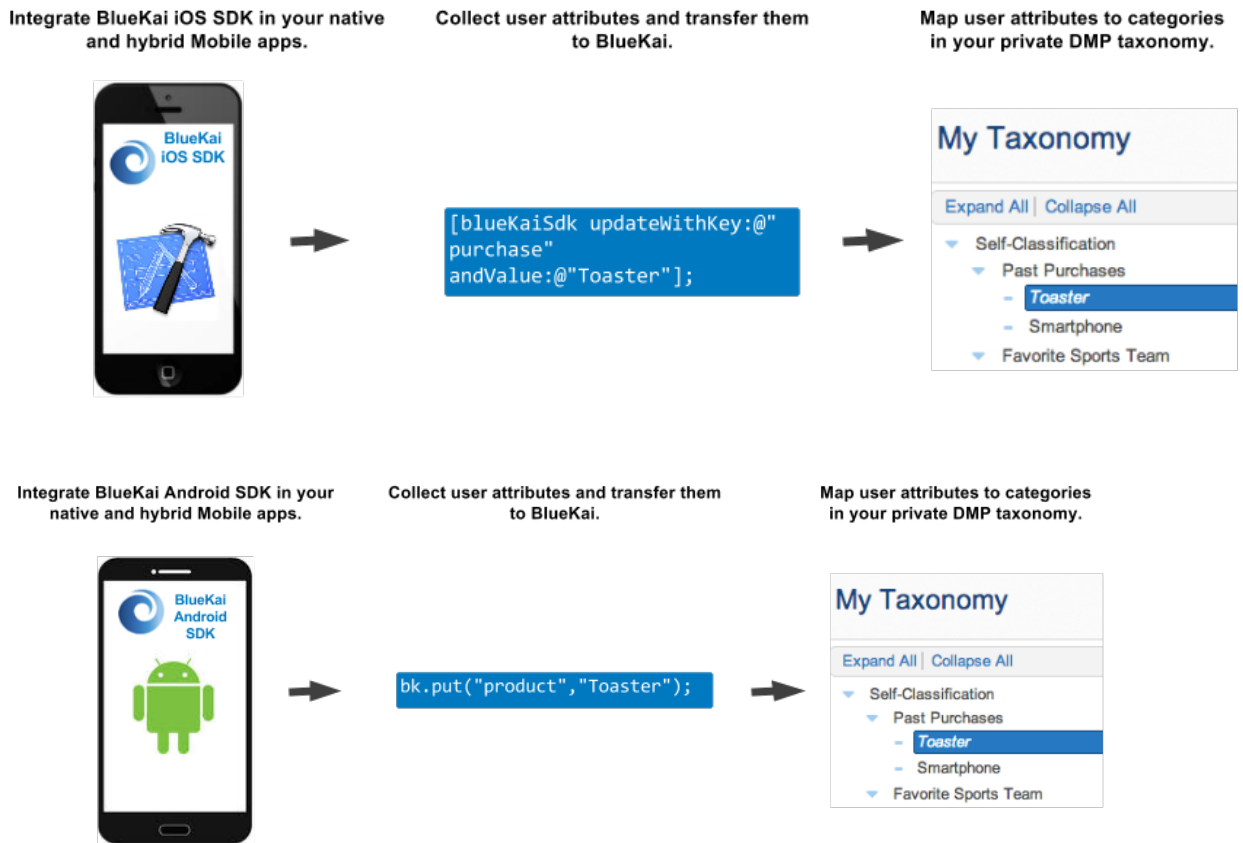
Tracking, The Web Conference (April 19-23, 2021), https://www3.cs.stonybrook.edu/~mikepo/papers/firstparty.www21.pdf [https://perma.cc/W3MH-GU8X].

[72] *iOS SDK*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/MobileIntegrations/ios_sdk.html [https://perma.cc/3475-3X3B].

[73] *Android SDK*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/MobileIntegrations/android_sdk.html [https://perma.cc/GB3K-ELJA].

[74] Using a Private ID Graph, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/IDManagement/private_id_setup.html [https://perma.cc/U2YD-F4T8].

[75] Joseph Cox, *Inside the Industry That Unmasks People at Scale*, Vice, (July 14, 2021), https://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii [https://perma.cc/TZ64-ECAG].

1

66.   Oracle's marketing materials[76] make explicit that Oracle's ID Graph "Unites All

2

Interactions Across Various Channels to Create One Addressable Consumer Profile":

15
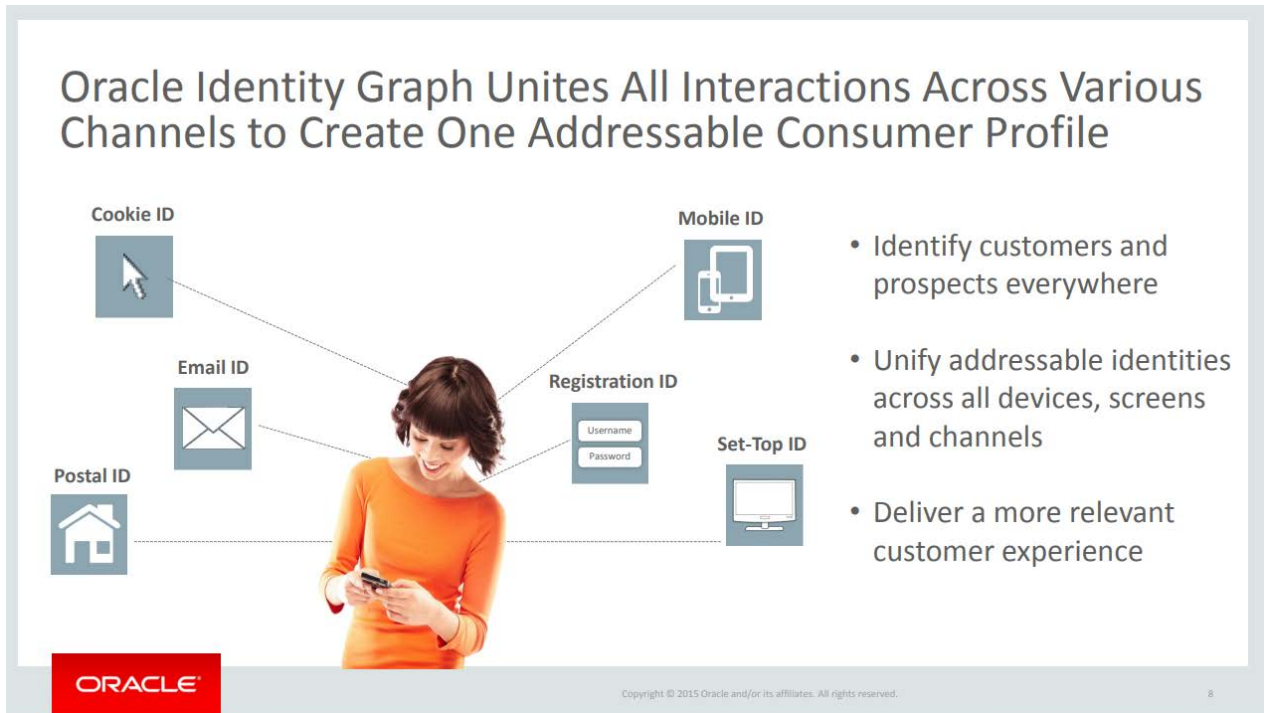
67.   A 2019 investigation into Oracle's profiling activities[77] resulted in the following

16

analysis demonstrating the all-encompassing nature of the online and offline data Oracle collects

17

and associates with IDs, which are tied to individual Class members, including information related

18

to credit card purchases from Visa and MasterCard, brick-and-mortar establishments, and credit

19

reporting agencies:

---

[76] *Oracle Buys Datalogix*, Oracle (Jan. 23, 2015),
https://web.archive.org/web/20200807021726/https://www.oracle.com/us/corporate/acquisitions/
datalogix/general-presentation-2395307.pdf [https://perma.cc/MQR4-5UEC].

[77] Wolfie Christl, *Corporate Surveillance in Everyday Life,* Cracked Labs (Jun. 2017),
https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf
[https://perma.cc/T7Z6-JPZK].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS
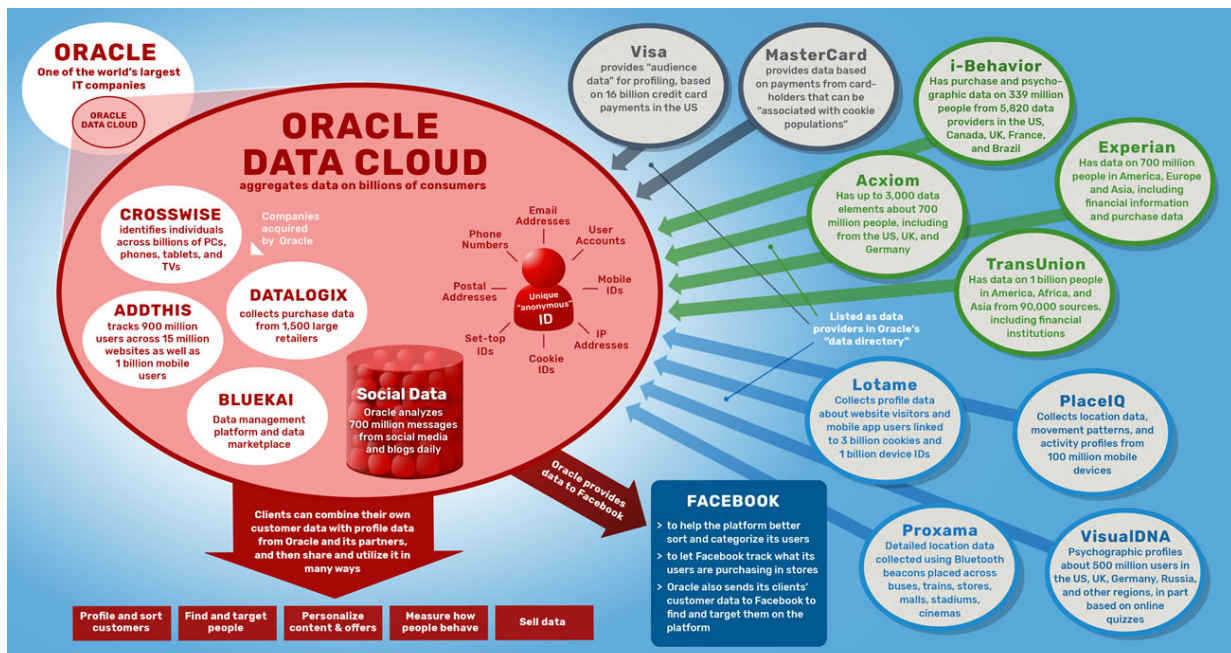
© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information, mainly the companies' own statements. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Oracle website, press releases, data directory, brochures, presentations. MasterCard website. Acxiom annual report. TransUnion annual report. Lotame website. VisualDNA brochure. Facebook website. ProPublica article. For details about the sources see the report "Corporate Surveillance in Everyday Life".

68.   In 2016, approximately one year after launch, Oracle Chairman and Chief Technological Officer Larry Ellison boasted there were five billion people in Oracle's ID Graph.[78]

69.   According to Ellison, the purpose of Oracle ID Graph is to predict and influence the future behavior of billions of people. He explained Oracle could achieve this goal by looking at social activity and locations in real time, including "micro location[s]." For example, Ellison has represented that companies will be able to know how much time someone spends in a specific aisle of a specific store and what is in the aisle of the store. "By collecting this data and marrying it to things like micro location information, Internet users' search histories, websites visits and product comparisons along with their demographic data, and past purchase data, Oracle will be able to predict purchase intent better than anyone."[79]

70.   Ellison likened the breadth and detail of Oracle's data collection to Facebook's— even arguing Oracle is better at mass surveillance and profiling than Facebook:

> Now where does this demographic data come from? Where does this past purchasing stuff come from? Well Oracle Data Cloud is the world's largest data

---

[78] Andrew Birmingham, *Oracle Has Five Billion Consumers In Its Identity Graph: Ellison*, Linkedin (Sept. 19, 2016) https://www.linkedin.com/pulse/oracle-has-five-billion-consumers-its-identity-graph-birmingham [https://perma.cc/MZ57-C4UN].

[79] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

base. There are two big databases to keep track of consumers and which have a lot of information about consumers. One is very famous, it's called Facebook. The other one is less well known, it's Oracle's Data Cloud . . .They have great data, don't get me wrong. Facebook has incredible data assets, but so do we. In our data cloud marketers are able to target consumers and do a much better job at predicting what they're going to buy next.[80]

71.   Ellison's vision for mass surveillance and profiling is totalizing and extends to the entire world: "How many people are on earth? Seven billion, two billion to go."[81]

C.   Oracle Uses the Data Marketplace to Enrich the Dossiers It Compiles on Class Members.

72.   Oracle, its partners, and its customers work in parallel to compile personal data and associate that data with specific individuals, effectively creating "dossiers" on people across the world. Oracle accomplishes its dossier building through its multifarious business practices, including not only the functionality of the Oracle ID Graph that connects, unifies, and then associates data to a person into a "profile," but also the functioning of the Oracle Data Marketplace. Oracle's Data Marketplace is an online store owned and operated by Oracle where Oracle facilitates the buying and selling of data and data-derived services by Oracle and its so-called "premier partners" to private, commercial, and governmental entities. The Data Marketplace allows the confluence of mass amounts of personal data by which its participants, including Oracle, can continually track people's activities and enrich people's dossiers.

73.   The Data Marketplace trades in (1) personal data that Oracle collects itself such as that collected via BlueKai tracking pixels (first-party data); (2) personal data that private companies collect from their own users and sell directly to Oracle clients (second-party data); and (3) personal data that other third-party data brokers collect and sell to Oracle clients on the Data Marketplace (third-party data).

1.   Oracle Audiences.

74.   Oracle Audiences are derived from the raw personal information that Oracle itself collects from Internet users via the cookies, tracking pixels, cross-device tracking, AddThis, and

---

[80] *Id.*
[81] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   Datalogix technologies described above.[82]   Oracle takes this personal information and applies

2   algorithmic processing to develop inferences about specific people. Oracle uses the inferences it

3   has made to assign people to certain "audiences" or segments.

4   75.   For example, for Mother's Day, Oracle's marketing materials explained that

5   Oracle's proprietary audience segments could help marketers target the following groups: (1)

6   "Millennials spoil moms," 24-35 year olds who Oracle predicted were going to purchase higher

7   priced gifts such as jewelry or electronics, (2) "Breakfast at Tiffany's," or people who were "more

8   likely to spring for earrings over roses," and (3) "Mama's boys," 18-24 year old men who were

9   likely going to buy an expensive gift for their mother.[83]   Oracle touts that Oracle Audiences are

10 effective because "the best predictor of future behavior is past behavior."

11   76.   Oracle's Health and Wellness segments reveal sensitive, health-related types of

12 personal information Oracle collects on Class members. By way of example only, these segments

13 include individuals struggling with insomnia ("Sleeping aids"), acne ("Acne Treatments"), weight

14 issues ("Diet Programs," "Weight Loss Programs," and "Adult Nutrition & Weight Control"), and

15 nicotine addiction ("Smoking cessation").[84]

16   **2.   Second-party data.**

17   77.   Oracle also facilitates the sale and purchase of second-party data, i.e., personal

18 information collected from Internet users by one company and sold directly to another company.

19 Data buyers can browse the second-party data listings on the Data Marketplace and contact data

20 sellers.[85]   These direct deals occur in a closed, private market operated by Oracle: "The data seller,

21

22 [82] *Oracle Audiences*, Oracle, https://www.oracle.com/cx/advertising/audiences/
    [https://perma.cc/C9TV-QUAW].

23 [83] *Give Your Mother's Day Campaigns the Special Treatment*, Oracle,
    https://www.oracle.com/a/ocom/docs/cx-mothers-day-audience-data.pdf [https://perma.cc/8QBP-

24 86NF].

25 [84]*Health and Wellness Preference Data Segments*, Oracle,
    https://www.oracle.com/us/assets/health-data-segments-020715-2537890.pdf

26 [https://perma.cc/9FWJ-AUJM].

27 [85] *Using the Second-party Data Discovery Marketplace*, Oracle,
    https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-
    center/Platform/ManagingTaxonomy/second-party_data_marketplace.html

28 [https://perma.cc/464C-R426].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                       CASE NO. 3:22-CV-04792-RS

1 buyer, and Oracle can then work together to make a deal."[86] After purchase, buyers can enhance

2 the ID Graph by uniting the second-party data with other personal information in the ID Graph,

3 thereby painting a more specific and detailed picture of Internet users.

3.   Other Data Brokers (Third-party data).

5   78.   Oracle operates the world's largest third-party data marketplace.[87] Third-party data

6 is information collected by companies that do not have a direct relationship with Internet users.

7 Data brokers participating in Oracle's Data Marketplace freely portray themselves as able to defeat

8 users' anti-tracking precautions, a pitch at odds with Oracle's privacy policies and its professed

9 respect for the right of individuals to opt out. For instance, ALC Real World Data, a "branded

10 data provider[] available through the BlueKai Marketplace" that offers "political" data, claims to

11 provide "a deeper understanding of the people you're targeting" because it "has no cookies to

12 erase and can't be 'cleared.'"[88]

13   79.   Oracle partners with over 65 major brokers of third-party data and refers to these

14 companies as "Branded Data Providers."[89] The personal information sold by Branded Data

15 Providers on the Oracle Data Marketplace can be used to enhance the digital dossiers in the Oracle

16 ID Graph.[90] A number of Oracle's Branded Data Providers sell highly intrusive and offensive

17 personal information without consent:

18   a.   Mobilewalla: Boasts of having "billions of data points daily" from 276

19 million unique mobile devices in the U.S. alone[91], and 1.5 billion mobile devices in 31 countries

20

21 [86] *Id.*

[87] *Oracle Data Marketplace,* Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-
22 help-center/AudienceDataMarketplace/AudienceDataMarketplace.html [https://perma.cc/27S8-
GX7H].

23 [88] *2019 Data Directory*, Oracle (2019),
https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-
24 directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

[89] *Branded Data Providers*, Oracle, https://www.oracle.com/cx/advertising/data-providers/
25 [https://perma.cc/7VBG-34XD].

[90] *Get o the Heart of the Matter, the Heart of Your Customer*, Oracle,
26 https://www.oracle.com/assets/brochure-data-driven-marketing-odc-2894231.pdf
[https://perma.cc/3W3X-JYC7].
27
[91] *Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives
28 Matter Demonstrators*, House Committee on Oversight and Reform, Chairwoman Carolyn B.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 worldwide.[92] In particular, Mobilewalla sells age, gender, GPS, and location data. Mobilewalla

2 specifically advertises the personal location information it sells as a way to increase political

3 campaign results.[93] During the summer of 2020, Mobilewalla tracked mobile devices to collect

4 data on 17,000 Black Lives Matter protesters including their home addresses and demographics.

5 Mobilewalla also released a report entitled "George Floyd Protester Demographics: Insights

6 Across 4 Major US Cities," which prompted a letter and investigation by Senator Elizabeth

7 Warren and other congress members.[94] In response to this investigation, Mobilewalla revealed

8 that it had provided location data used by the Department of Homeland Security, the Internal

9 Revenue Service, and the U.S. military for warrantless tracking of devices both at home and

10 abroad.[95]

11   b.   140 Proof: Collects data from 700-plus million social media users across

12 various social networks. The data includes content as well as meta-data such as "follows, check-

13 ins, re-blogs, pins, likes, or share." It claims to be able to build and target audiences for "hard to

14 find users" and "social influencers."[96]

15   c.   Affinity Answers: Advertises data on Class members' interests in political

16 organizations (e.g., NAACP, National LGBTQ Task Force, Planned Parenthood), political media

17 figures (e.g., Bill O'Reilly, Glenn Beck, Anderson Cooper, Arianna Huffington), state-level

18

19 Maloney, (Aug. 4, 2020) https://oversight.house.gov/news/press-releases/warren-maloney-
    wyden-desaulnier-probe-data-brokers-collection-of-data-on-black [https://perma.cc/VKW2-
20 NQSK].

    [92] *What is Geo-Behavioral Advertising?*, Mobilewalla (Feb. 8, 2019),
21 https://www.mobilewalla.com/blog/what-is-geo-behavioral-advertising [https://perma.cc/N9H2-
    YTRC].

22 [93] *Audience Segments*, Mobilewalla, https://www.mobilewalla.com/products/audience-segments
    [https://perma.cc/KW4D-H5F7].

23 [94] John Donegan, *The Incessant Surveillance by Data Brokers Needs to be Addressed*,
    ManageEngine (Oct. 6, 2021), https://insights.manageengine.com/privacy-compliance/the-
24 incessant-surveillance-by-data-brokers-needs-to-be-addressed/ [https://perma.cc/F8HX-ZPHF].

    [95] Bryan Tau, *How Cellphone Data Collected for Advertising Landed at U.S. Government
25 Agencies,* The Wall Street Journal (November 18, 2021, 8:30 AM ET),
    https://www.wsj.com/articles/mobilewalla-says-data-it-gathered-from-consumers-cellphones-
26 ended-up-with-government-11637242202 [https://perma.cc/S6AB-93XY].

27 [96] *Oracle Data Cloud Data Directory*, Oracle,
    https://web.archive.org/web/20180501185159/http://oracle.com/us/solutions/cloud/data-directory-
28 2810741.pdf [https://perma.cc/ANG8-H277].

SECOND AMENDED CLASS ACTION COMPLAINT
                                         CASE NO. 3:22-CV-04792-RS

1   Democratic Party and Republican Party organizations, and specific politicians in office.[97] It

2   harvests information about hundreds of millions of users from major social networks such as

3   Facebook, Instagram, and Twitter.

4   d.   Gravy Analytics: Advertises location intelligence at "millions of places,

5   points-of-interest and local events" to power "precision-targeted mobile advertising campaigns."

6   Its "Brand Audiences" include 2000-plus U.S. chain locations such as BestBuy, Burger King,

7   Starbucks, and Target.[98] It also sells phone location data to government agencies.[99] Indeed, the

8   FBI contracts with Gravy Analytics' subsidiary, Venntel, for the monitoring of social media posts

9   and location data. In 2020, the House Committee on Oversight and Reform opened an

10   investigation into Venntel for its business of buying location data from various smartphone apps

11   and selling that data to agencies including the FBI, Department of Homeland Security, DEA, ICE,

12   CBP, and the IRS. The Trump Administration also used Gravy Analytics' location data to track

13   people crossing the US-Mexico border.

14   e.   Acxiom: This massive data broker openly and explicitly advertises that it

15   has data on 45.5 million current and former U.S. military personnel.[100]

16

17

[97] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, Duke University
18   Sanford Cyber Policy Program (2021), https://sites.sanford.duke.edu/techpolicy/wp-
     content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-
19   2021.pdf [https://perma.cc/34SV-XY6M].

[98] *Gravy Analytics Unveils Location Data Forensics*, Gravy Analytics (Dec. 19, 2018),
20   https://gravyanalytics.com/press/gravy-analytics-unveils-location-data-forensics/
     [https://perma.cc/SE3K-KMSH]; *Location-Based Advertising: Brand Audiences*, Gravy Analytics
21   (Mar. 26, 2018), https://gravyanalytics.com/blog/location-based-advertising-branded-audiences/
     [https://perma.cc/4C4B-PSYP]; *Paramount, Best Buy & Gravy Analytics: Consumer Insights for
22   Advertising*, Gravy Analytics, https://gravyanalytics.com/paramount-best-buy/
     [https://perma.cc/E8UU-H6AY] ; *Starbucks & the Pumpkin Spice Latte: Using Location Data to
23   Measure Foot Traffic*, Gravy Analytics, (Aug. 21, 2019),
     https://gravyanalytics.com/blog/starbucks-the-pumpkin-spice-latte-using-location-data-to-
24   measure-foot-traffic/ [https://perma.cc/9PVQ-ME55].

[99] Lee Fang, *FBI Expands Ability To Collect Cellphone Location Data, Monitor Social Media,
25   Recent Contracts Show*, The Intercept (Jun. 24, 2020, 11:56 AM),
     https://theintercept.com/2020/06/24/fbi-surveillance-social-media-cellphone-dataminr-venntel/
26   [https://perma.cc/MJ58-QL3Z].

[100] Justin Sherman, *Data Brokers Are Advertising Data on U.S. Military Personnel*, Lawfare
27   (Aug. 23, 2021), https://www.lawfareblog.com/data-brokers-are-advertising-data-us-military-
     personnel [https://perma.cc/LHP5-ZK2G].

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                                                        CASE NO. 3:22-CV-04792-RS

1   f.   Eyeota: At least as of December 8, 2021, Dun & Bradstreet subsidiary

2   Eyeota offered a vast range of sensitive categories.[101] These include national security categories

3   described as "People who work in the Navy," "in the Marines," "in the Army," "in the Air

4   Force," "in the Coast Guard," "in the military," "in the Pentagon" "in law enforcement," "in [the]

5   judiciary," "in government," and one for "Elected Officials." Even former service members are

6   targeted; the "Military DoD" category applies to "Professionals who have honorably served or are

7   currently serving in the military."[102] Eyeota also provides categories that could be used to

8   influence these individuals, such as "Substance Abuse," "Alcohol," "Gamblers," "Payday Loans,"

9   "Debt," and "Welfare and Unemployment."[103] Nor are politics and health off limits. Eyeota

10 offers political categories like "Republican," "Leans Right," "Conservative," "Libertarian,"

11 "Eligible Voters," "Likely Voter," "Likely Gun Owners," "FOX NEWS," and "Oppose Raising

12 Taxes." Health categories include "Heart Disease," "Diabetes," "Chronic Pain," "Chronic Fatigue

13 Syndrome," "Sleep Disorders," "Panic / Anxiety Disorders," "Depression," "Psychology /

14 Psychiatry," "Physical Therapy," and "Surgery."[104] On information and belief, these sensitive

15 segments were for sale on the Data Marketplace.

16   80.   Oracle provides, and profits from, this data marketplace that allows third-party data

17 brokers to traffic in Class members' highly sensitive personal information. The following

18 examples non-exhaustively illustrate the types of sensitive information Oracle facilitates the sale

19 of in its Data Marketplace:

20

21

---

22 [101] *Eyeota RTB segment list (global), December 2021*, Irish Council for Civil Liberties
    (November 17, 2023), https://www.iccl.ie/wp-content/uploads/2023/10/Doc-2-as-printed-Eyeota-
23 8-December-2021.pdf [https://perma.cc/8C8H-L8RS]. The Eyeota category list was originally
    downloaded on December 8, 2021, and is one of the sources of a recent security report by the
24 Irish Council for Civil Liberties. *America's Hidden Security Crisis*, Irish Council for Civil
    Liberties (November 14, 2023), https://www.iccl.ie/digital-data/americas-hidden-security-crisis/
25 [https://perma.cc/EEB5-A4UV].
26 [102] *Eyeota RTB segment list (global), December 2021*, Irish Council for Civil Liberties
    (November 17, 2023), https://www.iccl.ie/wp-content/uploads/2023/10/Doc-2-as-printed-Eyeota-
27 8-December-2021.pdf [https://perma.cc/8C8H-L8RS].
    [103] *Id.*
28 [104] *Id.*

- 37 -   SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

1   a.   *Race*: At least five data brokers expressly provide racial categories as

2   "audience segments." These include "African American," "Asian," "Hispanic," "Caucasian," and

3   "American Indian."[105] Multiple data brokers' (e.g., Retargetly, DataXpand) business model

4   consists entirely of targeting Hispanic audiences.[106]

5   b.   *Location*: Data brokers offer location tracking, including a "real-time GPS

6   signal." Mobilewalla, for instance, described above, has advertised to Oracle customers that its

7   data can be used to serve a person an ad "at a specific time (say between 8-8:30PM), at a specific

8   location/place (say at the AT&T Stadium in Dallas) during a specific event (say, a country music

9   concert by Shania Twain)."[107] Cuebiq advertises "precise location data" from 61+ million U.S.

10 smartphone users on over 180 mobile apps.[108] TrueData advertisers "real-time GPS and beacon

11 location signals" on 245 million U.S. mobile users.[109]

12   c.   *Politics*: Data brokers participating in Oracle's Data Marketplace purport to

13 offer segments based on detailed political information, and some are avowedly partisan in doing

14 so. i360, for example, bills itself as "the leading data and technology resource for the pro-free-

15 market political and advocacy community" with a database of "199 million voters from all 50

16 states."[110] It boasts a dataset that includes "extensive political identification, coalition and

17

18 [105] *2019 Data Directory*, Oracle (2019),
    https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-
19 directory-2810741.pdf [https://perma.cc/EV8L-PG7V].
    [106] *Helping You Understand and Reach Latin American Consumers Through Digital*, Retargetly,
20 https://retargetly.com/ [https://perma.cc/PS4C-JQR9].
    [107] Anindya Datta, *A largely Ignored But Critical Dimension to Incorporate in Understanding
21 Consumers on Mobile. The Data Source, Inspired Thinking on our Data-Driven World*. Oracle
    (Fall 2016), https://cdn2.hubspot.net/hubfs/4309344/the-data-source-magazine-fall-2016.pdf
22 [https://perma.cc/ZZ8S-5RBK].
    [108] *Cuebiq and Drawbridge Double-Down on Cross-Device Reach & Attribution*. Cuebiq.
23 https://www.cuebiq.com/press/cuebiq-drawbridge-reach-attribution/ [https://perma.cc/GK4T-
    V8FX].
24 [109] *Holiday Campaign Planner: 3 Critical Strategies to (Re)Connect to Retail Mobile Customers*,
    TrueData, https://www.truedata.co/holiday-campaign-planner-3-critical-strategies-to-reconnect-
25 to-retail-mobile-customers/ [https://perma.cc/8ALU-6DHZ].
    [110] *comScore and i360 Team Up to Provide Digital Marketing Insights for Political Campaigns
26 and Advocacy Groups*, Cision PR Newsire (Apr. 17, 2012), https://www.prnewswire.com/news-
    releases/comscore-and-i360-team-up-to-provide-digital-marketing-insights-for-political-
27 campaigns-and-advocacy-groups-147750205.html [https://perma.cc/4F88-VHPT]; *The Database,
    Individual-Centric Data Warehouse*, i-360, https://www.i-360.com/the-database/
28

SECOND AMENDED CLASS ACTION COMPLAINT
                                                CASE NO. 3:22-CV-04792-RS

1   membership information collected by way of in-person, phone and online surveys, as well as

2   through partner relationships in addition to lifestyle and consumer data collected from multiple

3   top-tier providers."[111] It advertises registration and partisanship segments such as "Catholic,"

4   "Pro 2nd Amendment," "Pro Choice," "Pro Life," "Pro Marriage Same Sex," "Pro Traditional

5   Marriage," "Democratic Voters," "Independent Voters," "Republican Voters," "Swing Dem

6   Voters," and "Swing GOP Voters."[112] As noted above, Eyeota also offers extensive political

7   segments for sale.

8   d.   *Medical*: OnAudience, a "data provider" that profiles Internet users by

9   "observing user activity based on websites visited, content consumed and history paths to find

10   clear behavior patterns and proper level of intent,"[113] lets customers target individuals categorized

11   as interested in "Brain Tumor," "AIDS & HIV," "Substance Abuse" and "Incest & Abuse

12   Support."[114]

13   81.   Oracle monetizes Class members' personal information in part by providing a

14   process through which Oracle clients can winnow Oracle's vast store of detailed user data into

15   fine-grained audiences. For instance, an Oracle client could choose to filter billions of people

16   down to a handful of Class members who fit a cross-section of micro-targeted segments. Oracle

17   also allows clients to create audiences that exclude based on any or all of the same criteria.

18   82.   Based on Oracle's public-facing documentation, Oracle provides detailed "control

19   panels" to its clients which allows the clients to analyze, segment, and target Plaintiffs and Class

20   members based on the digital dossiers Oracle has compiled on them[115]:

21   _____

[https://perma.cc/8TY2-C9HH].

22   [111] *The Database, Individual-Centric Data Warehouse*, i-360, https://www.i-360.com/the-database/ [https://perma.cc/8TY2-C9HH].

23   [112] *Data Dictionary, Online Segments*, I-360, https://www.i-360.com/wp-content/uploads/2019/03/i360-Online-Segment-Data-Dictionary.pdf [https://perma.cc/392Q-3RFL].

24

25   [113] *2019 Data Directory*, Oracle (2019), https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

26

27   [114] Dr. Johnny Ryan, *Submission to the Irish Data Protection Commission*, Irish Council for Civil Liberties (Sept. 21, 2020), https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf [https://perma.cc/Y2J6-Z9YF].

28   [115] *Creating Audiences*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Platform/Audiences/create_audience.html [https://perma.cc/K6F2-NPZF].

SECOND AMENDED CLASS ACTION COMPLAINT
                                        CASE NO. 3:22-CV-04792-RS

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

83.   In other words, Oracle facilitates the creation of proxies for protected classes like

race, and allows its clients to exclude on that basis. For example, one Oracle customer website

describes how, after Facebook made it more difficult to target ads based on race in the

employment and credit areas, Oracle helped it achieve the same result.[116]

84.   Oracle clients include not only businesses looking to advertise their wares, but also

political campaigns and government agencies seeking to surveil, investigate, or target particular

individuals with propaganda. Oracle markets directly to these public agencies and political

parties, and refers to them as "Public Sector Customers."

85.   Political campaigns now have "needle-in-the-haystack capabilities" to "microtarget

voters on all their devices" using personal information sold by data brokers.[117] The Trump

---

[116] *Natural Intelligence Secures Higher Quality Purchases Using Oracle Audiences Within Skai*™, Skai, https://skai.io/case-studies/natural-intelligence-secures-higher-quality-purchases-using-s-third-party-audiences/ [https://perma.cc/UT5C-VQTU].

[117] Jeff Chester, *Our Next President: Also Brought to You by Big Data and Digital Advertising*, Bill Moyers (Jan. 6, 2017), https://billmoyers.com/story/our-next-president-also-brought-to-you-by-big-data-and-digital-advertising/ [https://perma.cc/R8FE-9J9W].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 campaign, for example, built a 220 million–person database of voter information named "Project

2 Alamo" using Datalogix, a data collection platform owned by Oracle. [118] Project Alamo, powered

3 by Oracle data, facilitated the Trump campaign's voter suppression initiatives including highly

4 targeted political advertising to African Americans, white women, and young white liberals[119] in

5 16 swing states, several of which were narrowly won by Trump. In Michigan, a state that Trump

6 won by only 10,000 votes, 15% of voters are black, but they represented 33% of Project Alamo's

7 "special deterrence" category.[120] These voters received anti-Clinton Facebook ads that included

8 audio of Hilary Clinton referring to African-American children as "superpredators."[121] Through

9 Project Alamo's voter suppression efforts, it is estimated that 2 million black voters who voted in

10 2012 did not vote in 2016.[122]

11 　　　86.　　　Oracle also powers "Facebook Custom Audiences" which allows advertisers,

12 including political parties and campaigns around the world, to push ads to Facebook using

13 personal data unlawfully collected and sold by Oracle.[123] Oracle also recently announced a

14 partnership with Amazon: Oracle Audiences is now integrated into the Amazon platform allowing

15 Oracle's clients to target Amazon users.[124]

16

[118] Nina Burleigh, *How Big Data Mines Personal Info to Craft Fake News and Manipulate Voters*, Newsweek (Jun. 8, 2017, 1:01 PM), https://www.newsweek.com/2017/06/16/big-data-mines-personal-info-manipulate-voters-623131.html [https://perma.cc/6DZ4-WYD9].

[119] Joshua Green & Sasha Issenberg, *Inside the Trump Bunker, With Only Days to Go*, Bloomberg (Oct. 27, 2016, 3:00 AM PDT), https://www.bloomberg.com/news/articles/2016-10-27/inside-the-trump-bunker-with-12-days-to-go [https://perma.cc/9RN2-WCKS].

[120] Dan Sabbagh, *Trump 2016 Campaign 'Targeted 3.5m Black Americans to Deter them From Voting'*, The Guardian, (Sept. 28, 2020, 1:24 PM EDT), https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting [https://perma.cc/W4GX-UHTN].

[121] Andrew Marantz, *The Man Behind Trump's Facebook Juggernaut*, The New Yorker (Mar. 2, 2020), https://www.newyorker.com/magazine/2020/03/09/the-man-behind-trumps-facebook-juggernaut [https://perma.cc/TE8H-DTR5].

[122]Dan Sabbagh, *Trump 2016 Campaign 'Targeted 3.5m Black Americans to Deter them From Voting'*, The Guardian, (Sept. 28, 2020, 1:24 PM EDT), https://www.theguardian.com/us-news/2020/sep/28/trump-2016-campaign-targeted-35m-black-americans-to-deter-them-from-voting [https://perma.cc/W4GX-UHTN].

[123] *Find Buyers at Scale on Facebook With Oracle Data*, Oracle, https://www.oracle.com/a/ocom/docs/six-steps-activating-odc-audiences-on-facebook.pdf [https://perma.cc/G7R5-5CJM].

[124] Rob Tarkoff, *Oracle and Amazon Advertising Help Advertisers Engage Online Shoppers*, Oracle Blog (Jun. 2, 2021), https://www.oracle.com/news/announcement/blog/oracle-amazon-

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

87.   The general public does not have access to the Data Marketplace, or any visibility into who is buying and selling their information. Access is restricted to buyers and sellers, so individuals whose data is being bought and sold have no reasonable insight into what occurs there or the extent of Oracle's violations of their privacy rights. Publicly available information indicates that data sold on the Data Marketplace is highly sensitive, and is collected in pernicious and illegal ways.

88.   Oracle does not publicly disclose the identity of its clients that participate on the Data Marketplace. Plaintiffs and Class members have no reasonable basis to discern the identity of the persons and/or entities that buy or sell information about them on the Data Marketplace.[125] This opacity extends to possible state actors. Oracle has a well-documented history of marketing its technology to state actors within the United States and abroad.[126] While Oracle *does* have a total embargo on data sales to a small group of countries including Iran, North Korea, and Syria,[127] it has marketed its surveillance products to governments, police or paramilitary forces, including China,[128] Brazil, Mexico, Pakistan, and the United Arab Emirates.[129]

---

advertising-help-advertisers-engage-shoppers-2021-06-02/ [https://perma.cc/L864-A2EA].
[125] Nor, for that matter, does Oracle disclose what process it uses to vet Data Marketplace participants.
[126] *Government and Education*, Oracle, https://www.oracle.com/industries/government/ [https://perma.cc/J5NN-E97U].
[127] *Data Restrictions*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-center/Introduction/Privacy/embargo.html [https://perma.cc/NQ83-FJUP].
[128] Mara Hvistendahl, *How Oracle Sells Repression in China*, The Intercept (Feb. 18, 2021, 3:20 AM), https://theintercept.com/2021/02/18/oracle-china-police-surveillance/ [https://perma.cc/W45L-RGTE]; Mara Hvistendahl, *How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"*, The Intercept (Apr. 22, 2021, 12:00 AM) https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/ [https://perma.cc/RXJ6-38VD]; Mara Hvistendahl, *Oracle Executive's Contentious Interview with the Reporter He Sought Dirt On*, The Intercept (Apr. 30, 2021, 10:06 AM), https://theintercept.com/2021/04/30/oracle-china-ken-glueck/ [https://perma.cc/Z9VW-QZAW]; Mara Hvistendahl, *Oracle Boasted That its Software Was Used Against U.S. Protesters. Then It Took the Tech to China,* The Intercept (May 25, 2021, 8:25 AM), https://theintercept.com /2021/05/25/oracle-social-media-surveillance-protests-endeca/ [https://perma.cc/9RXG-CF5M].
[129] Mara Hvistendahl, *How a Chinese Surveillance Broker Became Oracle's "Partner of the Year"*, The Intercept (Apr. 22, 2021, 12:00 AM), https://theintercept.com/2021/04/22/oracle-digital-china-resellers-brokers-surveillance/ [https://perma.cc/RXJ6-38VD].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

D.   Data Brokers Are a Recognized Threat to Individual Privacy.

89.   The California Consumer Privacy Act (CCPA) defines a data broker as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." Cal. Civ. Code § 1798.99.80. The CCPA requires a data broker to register with the Attorney General. Oracle is registered as data broker in California pursuant to the CCPA.

90.   The New York Times has described data brokers as "Big Brother-in-Law,"[130] noting that the copious information they compile on individuals is "fused and vetted by algorithm to form an ever-evolving, 360-degree view of U.S. residents' lives."[131] As described in the Financial Times, "[t]he explosive growth of online data has led to the emergence of the super data broker —*the 'privacy deathstars'*, *such as Oracle* . . . that provide one-stop shopping for hundreds of different data points which can be added into a single person's file . . . As a result, everyone now is invisibly attached to a living, breathing database that tracks their every move."[132]

91.   Legislators have recognized the privacy-invasive nature of data brokers' core business practices. The sale of Americans' information to foreign states is a source of increasing public concern. Senator Ron Wyden, for example, has cited fears about the sale of location data, credit card purchases, and web browsing to the People's Republic of China as the impetus for a bill—the Protecting Americans' Data From Foreign Surveillance Act—that would largely bar the export of Americans' personal data.[133]

92.   Senator Wyden has also introduced the "Fourth Amendment is Not for Sale Act" to "put a stop to shady data brokers buying and selling Americans' Constitutional rights." The

---

[130] McKenzie Funk, *How ICE Picks Its Targets in the Surveillance Age,* The New York Times Magazine (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html [https://perma.cc/5678-ZEJX].

[131] *Id.*

[132] Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators try to Rein in the "Privacy Deathstars",* Financial Times (Jan. 8, 2019), ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521 [https://perma.cc/36DS-3R72] (emphasis added).

[133] *The Protecting Americans' Data From Foreign Surveillance Act,* Ron Wyden, United States Senator for Oregon, https://www.wyden.senate.gov/imo/media/doc/Protecting%20Americans%20Data%20from%20Foreign%20Surveillance%20Act%20of%202021%20One%20Pager.pdf [https://perma.cc/FS24-9XEB].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   proposed Act "closes the legal loophole that allows data brokers to sell Americans' personal

2   information to law enforcement and intelligence agencies without any court oversight – in contrast

3   to the strict rules for phone companies, social media sites and other businesses that have direct

4   relationships with consumers." As Senator Wyden explained:

5

6

7

> Doing business online doesn't amount to giving the government permission to
> track your every movement or rifle through the most personal details of your
> life … There's no reason information scavenged by data brokers should be treated
> differently than the same data held by your phone company or email provider. This
> bill closes that legal loophole and ensures that the government can't use its credit
> card to end-run the Fourth Amendment.[134]

8

9   93.   On December 8, 2021, Senator Wyden, in urging the Consumer Financial

10   Protection Bureau to take action against data brokers, stated:

11

12

> Data brokers are serving as shady middlemen to sell [consumers'] personal
> information without any legal protections . . . Selling personal information that
> people provide to sign up for power, water and other necessities of life, and giving
> them no choice in the matter, is an egregious abuse of consumers' privacy.[135]

13   94.   The FTC has recently warned consumers about the "shadowy" "data broker

14   ecosystem" where "companies have a profit motive to share data at an unprecedented scale and

15   granularity," including a "staggering" amount of "highly personal information that people choose

16   not to disclose even to family, friends, or colleagues."[136]

17   95.   In the wake of *Dobbs v. Jackson Women's Health Organization*, No. 19-1392, 142

18   S. Ct. 2228 (2022), the threat data brokers like Oracle pose to the privacy of individuals seeking

19   information about abortions is significantly magnified. An investigation recently revealed Oracle

20   trackers on the websites of nonprofits providing abortion resources and services, including

21

22   [134] *Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not For Sale Act,* Ron Wyden, United States Senator for Oregon (Apr. 21, 2021),

23   https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/LMP7-CWFU].

24   [135] *Wyden Urges CFPB to Protect Americans' Privacy and Stop the Sale of Personal Data by Credit Agencies,* Ron Wyden, United States Senator for Oregon,

25   https://www.wyden.senate.gov/news/press-releases/wyden-urges-cfpb-to-protect-americans-privacy-and-stop-the-sale-of-personal-data-by-credit-agencies [https://perma.cc/N777-6US8].

26   [136] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data,* The Federal Trade

27   Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use

28   [https://perma.cc/V6XT-85YX].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   Planned Parenthood.[137] Class members who have visited Planned Parenthood's website in states

2   where abortion is now illegal may have had their personal information tracked and compiled by

3   Oracle, which Oracle may then make available to law enforcement officials.

4   96.   Congressional representatives have expressed intense concern about law

5   enforcement officials using Oracle data to surveil and prosecute individuals researching abortion.

6   House Democrats recently sent Oracle a letter asking it to limit its sale of sensitive location

7   data.[138] Senators Elizabeth Warren and Wyden have also introduced the "Health and Location

8   Data Protection Act," which would ban data brokers like Oracle from selling health and location

9   data. As Senators Warren and Wyden state:

10   Data brokers profit from the location data of millions of people, posing serious
          risks to Americans everywhere by selling their most private information . . .
11   [w]hen abortion is illegal, researching reproductive health care online, updating a
          period-tracking app, or bringing a phone to the doctor's office all could be used to
12   track and prosecute women across the U.S. It amounts to uterus surveillance.[139]

13   97.   Consistent with Oracle's plan of engaging in wide-ranging surveillance of the

14   intimate health details of all Americans, Oracle's Larry Ellison has announced Oracle's plan to

15   build "a unified national health records database," which it is effectuating through its $28.3 billion

16   acquisition of electronic health record company Cerners. According to Ellison, Oracle is "building

17   a system where the health records [of] all American citizens[] . . . not only exist at the hospital

18   level but also are in a unified national health records database," apparently to be maintained and

19   controlled by Oracle.[140] Oracle plans to build this massive health database *prior to even*

20

21   [137] Alfred Ng & Maddy Varner, *Nonprofit Websites are Riddled with Ad* Trackers, The Markup
     (Oct. 21, 2021, 8:00 AM ET), https://themarkup.org/blacklight/2021/10/21/nonprofit-websites-
     are-riddled-with-ad-trackers [https://perma.cc/PW23-K5F2].

22   [138] Cristiano Lima, *Democrats Press Oracle, AWS Over Their Post-Roe Data Collection*, The
     Washington Post (July 21, 2022),
23   https://www.washingtonpost.com/politics/2022/07/21/democrats-press-oracle-aws-over-their-
     post-roe-data-collection/ [https://perma.cc/M4S9-CGDM].

24   [139] *Warren, Wyden, Murray, Whitehouse, Sanders Introduce Legislation to Ban Data Brokers
     from Selling Americans' Location and Health Data*, Elizabeth Warren, United States Senator for
25   Massachusetts (June 15, 2022), https://www.warren.senate.gov/newsroom/press-releases/warren-
     wyden-murray-whitehouse-sanders-introduce-legislation-to-ban-data-brokers-from-selling-
26   americans-location-and-health-data [https://perma.cc/J5XV-JFSR].

27   [140] Heather Landi, *Oracle, Cerner Plan to Build National Medical Records Database as Larry
     Ellison Pitches Bold Visionfor Healthcare*, Fierce Healthcare (June 10, 2022, 6:22 AM)
28   https://www.fiercehealthcare.com/health-tech/oracle-cerner-plan-build-national-medical-records-

                                          SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

purporting to obtain consent from patients: "Ellison said this new system will only have

anonymous information *until individual patients give consent.*"[141]

98.   Oracle has *itself* acknowledged the highly problematic nature of its own profile-

building conduct, albeit indirectly. Without a trace of irony, Oracle has argued to legislators both

in the U.S. and internationally that its business rival Google wrongfully builds "shadow profiles,"

"using massive amounts of consumer data, not all of which it discloses to consumers, to micro-

targe[t] advertising" to consumers without their consent. However, Oracle's description of

Google's conduct is a virtually word-for-word description of its own conduct as a data broker.

According to Oracle, Google's "shadow profiles" are:

> [M]assive, largely hidden datasets of online and offline activities. This information
> is collected through an extensive web of Google [*cf.* Oracle] services, which is
> difficult, if not impossible to avoid. *It is largely collected invisibly and without
> consumer consent.* Processed by algorithms and artificial intelligence, this data
> reveals an intimate picture of a specific consumer's movements, socio-economics,
> demographics, "likes," activities and more. It may or may not be associated with a
> specific users' name, but the specificity of this information defines the individual
> in such detail that a name is unnecessary.[142]

The hypocrisy of Oracle's lobbying efforts on this front has been noted by commentators in the

press.[143]

E.   Class Members Have Not and Cannot Consent to Oracle's Collection or Use of their Personal Information.

99.   The long-established common law, statutory, and Constitutional rights to privacy

are inherently and inextricably linked to fundamental cultural values of autonomy and freedom.

The concept of "consent" reinforces these cultural values by functioning as a way for individuals

to protect their privacy by exercising control over their personal information—what personal

---

database-ellison-pitches-bold-vision [https://perma.cc/G44G-77L6].

[141] Brody Ford, *Oracle's Ellison Pitches US Health Database With Power of Cerner*, Bloomberg (June 9, 2022, 2:35 PM PDT), https://www.bloomberg.com/news/articles/2022-06-09/oracle-s-ellison-pitches-national-health-database-on-cerner-deal [https://perma.cc/QB47-HYRG] (emphasis added).

[142] *Oracle Corporation Submission to the Digital Platforms Inquiry*, Oracle, https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF [https://perma.cc/LHE4-B47C].

[143] Mike Masnick, *Oracle's Projection: As It Accuses Google on Snooping on You, It Has Built a Huge Data Operation That it Doesn't Want Regulated*, techdirt (Apr. 9, 2021, 9:37 AM) https://www.techdirt.com/2021/04/09/oracles-projection-as-it-accuses-google-snooping-you-it-has-built-huge-data-operation-that-it-doesnt-want-regulated/ [https://perma.cc/X8WZ-ZUWJ] (emphasis added).

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   information organizations can collect, how they can use it, and to whom they can disclose it.

2   Oracle conducts the business practices alleged in this complaint within a context and in a manner

3   where consent from the persons whose data it assembles is not reasonably possible or practical, in

4   fact does not occur, and which in light of the extent of the privacy rights that are violated by

5   Oracle's business practices, no consent to such practices could be enforced as a matter of law.

6   100.   Plaintiffs and Class members, like our society at large, do not have the practical

7   choice or ability but to conduct their daily lives substantially in the digital world, connected to the

8   Internet, with their personal data traveling through cyberspace every day. Because much of daily

9   activities of life are now conducted online—whether financial, commercial, or social—Internet

10   activity has become an "exhaustive chronicle" of one's life. The personal data necessary for these

11   activities courses through the Internet as these activities take place, and, when aggregated, can

12   provide deep insight into a person's thinking, acting, and being. Without an expectation of privacy

13   on the Internet, there would functionally be no expectation of privacy anywhere.

14   101.   Oracle sits atop a complex data collection and processing apparatus feeding its

15   labyrinthine multinational data marketplace, making it impossible for ordinary persons to

16   reasonably understand the true purpose and extent of Oracle's data collection, compiling of digital

17   dossiers, and other data exploitation practices, which are opaque, if not invisible, to ordinary data

18   subjects. Given the complexity and disguised nature of Oracle's collection and use of personal

19   information, and the lack of any direct relationship between Oracle and the Plaintiffs and Class

20   members, there is no reasonable basis for Plaintiffs and the Class members to know the extent to

21   which Oracle is obtaining their data, tracking them, and selling their data or services derived from

22   their data.

23   102.   Oracle's presence on the Internet and in the digital world is ubiquitous, by design,

24   and its data gathering activities are constant, vast, and encompasses a massive swath of Internet

25   activity. The breadth and complexity of sources from which Oracle compiles digital dossiers, or

26   profiles, on Class members, including from credit card transactions and interactions with brick-

27   and-mortar establishments, is such that as a practical matter, Plaintiffs and Class members have no

28   way of knowing—and thus no way of even being able to consent to—the actual scope of Oracle's

1   conduct. Plaintiffs and Class members, do not, merely by virtue of conducting the necessary

2   activities of daily life, both online and in the physical world, consent to constant and pervasive

3   surveillance by Oracle and the creation of detailed dossiers about them.

4   103.   In as much as the Internet and digital existence has become integral to people's

5   lives, its functioning and complexity with respect to personal data remains opaque to reasonably

6   informed people. The Findings and Declarations of the California Privacy Rights Act (CPRA)

7   notes that the "asymmetry of information" inherent in the "collect[ion] and use [of] consumers'

8   personal information . . . makes it difficult for consumers to understand what they are exchanging

9   and therefore to negotiate effectively with businesses." There is asymmetry of knowledge

10 between Oracle and the data subjects it exploits, including Plaintiffs and the members of the Class,

11 in that Oracle has an complete knowledge of its data collection and data exploitation practices, but

12 Plaintiffs and Class members have no direct relationship with Oracle regarding these practices and

13 no reasonable basis to discern those practices nor the nature of the practices directed at them.

14   104.   Plaintiffs and Class members cannot reasonably foresee all the ways in which

15 Oracle may use the detailed dossiers it is compiling on them. Plaintiffs and Class members have

16 no way of knowing the specific third parties to which Oracle will provide their personal

17 information, or what those third parties will do with that information. Plaintiffs and Class

18 members thus cannot provide knowing and informed consent to Oracle's dissemination of their

19 personal information.

20   105.   Oracle makes no pretense of having directly obtained consent from the persons

21 whose data it gathers, including Plaintiffs and the Class members. At no point during its process

22 of collecting or processing personal data, or the compiling of dossiers or selling services based on

23 that personal data, does Oracle ever directly ask individuals for their consent. Oracle legally

24 acknowledges this by virtue of its registration as a data broker wherein it admits it "does not have

25 a direct relationship" with the subjects whose data it exploits. *See* Cal. Civ. Code § 1798.99.80.

26   106.   Nor have Plaintiffs and the Class members manifested any form of consent

27 indirectly to Oracle. Oracle publishes so-called privacy policies on its website, but these policies

28 are not reasonably directed to Plaintiffs and Class members, all of whom lack any direct

- 48 -   SECOND AMENDED CLASS ACTION COMPLAINT
                                   CASE NO. 3:22-CV-04792-RS

1   relationship with Oracle and have no reasonable insight into Oracle's data collection and data

2   exploitation practices or how they may or may not be subject to such practices, and therefore there

3   is no reasonable basis for Plaintiffs and Class members to be aware of Oracle's privacy policies or

4   to have directed themselves to them. Plaintiffs and the Class members are not legally subject to or

5   governed by Oracle's published privacy policies.

6   107.   Oracle's so-called privacy policies are themselves insufficient to adequately inform

7   Plaintiffs and the Class members about the nature and extent of Oracle's data collection and data

8   exploitation practices, even with regard to their personal data. Plaintiffs and the Class members

9   are in the course of daily life barraged with thousands of pages of purported "terms and

10 conditions" and "privacy policies" for online products and services. Computer science researchers

11 have estimated that, based on the number of unique sites American Internet users visit annually, it

12 would take the average Internet user between 181 to 304 hours to read the relevant privacy

13 policies; this translates to approximately 72 billion hours per year for every U.S. Internet user to

14 read all the privacy policies he or she encounters. Oracle knows, or reasonably should know, that

15 it is not reasonably possible for Internet users to read or comprehend the thousands of privacy

16 policies they encounter, including Oracle's privacy policies.

17   108.   As privacy scholars have noted, issues that users must navigate to understand the

18 significance of consent are too complex and the conditions surrounding consent too easy to

19 manipulate for any purported consent to be informed and meaningful.[144] While, as is well-known,

20 many websites include "cookie popups" that purport to ask for consent for the website placing a

21 cookie on the users' computer, in practice, most formulations of user control rights fail to

22 sufficiently explain that cookies tracking leads to *profiling* based on information *derived* from user

23 behavior. These practices, whether by Oracle or other third parties, fail to provide sufficient

24

25
      _____

26 [144] *See* Alessandro Acquisti, Curtis Taylor et al., *The Economics of Privacy*, 54 J. Econ. Literature
    442 (2016), https://pubs.aeaweb.org/doi/pdfplus/10.1257/jel.54.2.442 [https://perma.cc/3KPV-
    5WHV]; Woodrow Hartzog, Privacy's Blueprint: The Battle to Control the Design of New
27 Technologies (2018); Nora A. Draper & Joseph Turow, *The Corporate Cultivation of Digital
    Resignation*, 21 new media & soc'y (2019), https://doi.org/10.1177/1461444819833331
28 [https://perma.cc/J8B4-K3ES].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                  CASE NO. 3:22-CV-04792-RS

1   means to obtain the legally viable consent to Oracle's mass data collection, behavior tracking, and

2   assembling of dossiers based on that data.

3   109.   The content and organization of Oracle's privacy policies are convoluted, opaque,

4   and not reasonably comprehensible to the average Internet user. Oracle's website leads to *seven*

5   different privacy policies.[145] These privacy policies are sometimes complementary, sometimes

6   exclusive, and always vague about how they relate to one another. For example, the "Oracle

7   Advertising Privacy Policy," the "AddThis Privacy Policy," and the "Oracle General Privacy

8   Policy" all provide different and non-uniform information about how the company uses cookies,

9   leaving even an informed reader who seeks to educate themselves on how Oracle may be tracking

10   and using their data confused as to what exactly Oracle is doing.[146]

11   110.   Oracle's privacy policies fail to meaningfully disclose what Oracle does with

12   internet users' information. Oracle's so-called privacy policies fail to meaningfully disclose that

13   Oracle's customers pay to use Oracle's ID Graph, Data Marketplace, and related services which

14   Oracle promises will provide near-omniscience into the lives of Internet users.

15   111.   The Oracle Advertising Privacy Policy understates the depth of Oracle's

16   surveillance by failing to disclose its true range of categories of personal information that gives it

17   visibility into people's lives. This particular policy exclusively uses an example of an internet user

18   being targeted based on *one* characteristic: their interest in a Hawaiian vacation. Oracle's specific

19   example is "age bracket 25-55; adventurous traveler; surfing enthusiast; in market for travel

20   specials to Hawaii."[147] This sanitized illustration is impossible to square with the total visibility

21

---

22   [145] *See, e.g., Privacy @ Oracle*, Oracle, https://www.oracle.com/legal/privacy/privacy-policy.html [https://perma.cc/V848-G7BS] (described as the "General Oracle Privacy Policy," but also referring to the "Services Privacy Policy" for "information on how Oracle processes services

23   personal information.").
     [146] *Oracle Advertising Privacy Policy*, Oracle (version updated May 5, 2022),

24   https://www.oracle.com/legal/privacy/advertising-previous-privacy-policy-050522.html [https://perma.cc/MP25-TAXY]; *AddThis Privacy Policy*, Oracle version updated May 5, 2022),

25   https://www.oracle.com/legal/privacy/addthis-privacy-policy.html [https://perma.cc/E84S-W96V]; *Oracle General Privacy Policy*, Oracle (version updated May 5, 2022),

26   https://www.oracle.com/legal/privacy/previous-policy-050522.html [https://perma.cc/V848-G7BS].

27   [147] *Oracle Advertising Privacy Policy*, Oracle (version updated May 5, 2022),
     https://www.oracle.com/legal/privacy/advertising-previous-privacy-policy-050522.html

28   [https://perma.cc/MP25-TAXY].

SECOND AMENDED CLASS ACTION COMPLAINT
                                         CASE NO. 3:22-CV-04792-RS

1   into Internet users' lives that Oracle provides to clients, and the reality that the segments Oracle

2   offers regularly stretch to over a thousand categories.

3   112.   Oracle is also conspicuously silent about the Data Marketplace in its disclosures.

4   While the company touts the existence of "the world's largest third-party data marketplace" in

5   client-facing marketing materials, its privacy policies *do not even mention the Data Marketplace's*

6   *existence*. Although Oracle boasts elsewhere that the Data Marketplace hosts third parties who

7   sell internet users' sensitive personal data,[148] Oracle's privacy policies fail to disclose that Oracle

8   partners with other data brokers, nor provide the identity of these data broker partners.

9   113.   The Oracle Advertising Privacy Policy states that Oracle classifies "political …

10   orientation" as sensitive information, does not create "interest segments that reflect personal

11   information that we consider sensitive," and has "operational procedures … to prevent our partners

12   and customers from using personal information provided to them by Oracle to create interest

13   segments that we consider sensitive."[149] Any reasonable reader would infer from this that Oracle

14   does not facilitate the sale of their political views. In fact, the opposite is true: Oracle's

15   advertising materials highlight the fact that data brokers on the Data Marketplace sell data on

16   individuals' politics.[150]

17   114.   In practice, the "notice and consent" framework that permeates the Internet is

18   farcical. For example, a recent forensic investigation revealed that, in the context the IAB[151]

19   Europe "Transparency Consent Framework" (TCF), even when users specifically decline consent

20   to be tracked, various adtech participants—including Oracle—ignore those expressions of consent

21   ---

[148] *2019 Data Directory*, Oracle (2019),
22   https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-directory-2810741.pdf [https://perma.cc/EV8L-PG7V].
23   [149] *Oracle Advertising Privacy Policy*, Oracle (version updated May 5, 2022),
https://www.oracle.com/legal/privacy/advertising-previous-privacy-policy-050522.html
24   [https://perma.cc/MP25-TAXY].
[150]Oracle's professed decision to not selling political data is a recent development. As of 2016, its
25   marketing materials prominently advertised its data on individuals' political views. *The Audience Playbook, Inspiration for winning campaigns*, Oracle (Aug. 2016),
26   http://online.pubhtml5.com/mdhz/hgpp/#p=16 [https://perma.cc/4CUE-JKKV].
[151] The "Interactive Advertising Bureau (IAB) is an American advertising business organization
27   that develops industry standards, conducts research, and provides legal support for the online
advertising industry." Wikipedia, *Interactive Advertising Bureau*,
28   https://en.wikipedia.org/wiki/Interactive_Advertising_Bureau [https://perma.cc/FP9B-VE7B].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   and place trackers on users' devices.[152] The same study discovered that Oracle places tracking

2   cookies on a user's device *before the user even has a chance to decline consent*.[153] The IAB's

3   CCPA Framework is broadly similar to the European TCF, and is directed at Internet users in

4   California.[154]

5   115.   Neither Oracle's so-called privacy policies, or the policies of third party Internet

6   publishers, could provide any reasonable basis for Plaintiffs and Class members to have consented

7   to Oracle's data collection, compiling of digital dossiers, and other data exploitation practices, or

8   to have waived their privacy rights, including to be free from Oracle's pervasive surveillance of

9   them.

10   116.   Oracle knows, or reasonably should know, that Internet users such as Plaintiffs and

11   Class members have insufficient knowledge or basis to reasonably comprehend the extent to

12   which Oracle is obtaining their data, tracking their activity, and compiling it into digital dossiers,

13   nor the deeply invasive and detailed nature of those dossiers. Oracle makes no disclosure

14   anywhere directly to Plaintiffs or Class members of these practices. To the extent Plaintiffs or

15   Class members indirectly acknowledge to third parties the presence of some aspect of an isolated

16   data collection practice, or tracking cookie on an individual website, such acknowledgement in no

17   way does or could reflect any consent or sufficient understanding of Oracle's practices.

18

19   ---

[152] *Are Ad Tech Vendors in Europe Ignoring User Consent Signals?*, Adalytics,
20   https://adalytics.io/blog/adtech-not-checking-user-tcf-consent [https://perma.cc/W2R6-SUMY]
     ("Pierre's TCF string shows that he only consented to basic ads (and only from Google). He is
21   curious as to whether this ad creative that was served to his browser is indeed a "basic ad", devoid
     of any tracking or measurement pixels. He takes a look at the details of the "ad" attribute that
22   was sent in the HTTPS response. The Balenciaga ad contains tracking and ad viewability or
     render pixels from TripleLift, Google, Oracle Moat, and The Trade Desk.").
23   [153] *Id.* ("[A]nother EU citizen with a German IP address (we shall refer to them as "Charlotte"),
     creates a brand new Chrome instance, with no logins, cookies, local storage, or browser history.
24   Charlotte proceeds to visit reuters.com. As soon as Charlotte opens the Reuters landing page, she
     is shown a cookie consent banner from OneTrust. *Before Charlotte has a chance to make any*
25   *consent decisions or to read the consent text, several third party domains set cookies in*
     Charlotte's browser. We can observe Oracle Eloqua Marketing Automation ("eloqua.com") sets a
26   cookie called "ELOQUA GUID", which Oracle's documentation says is a "global unique
     identifier" to help personalize websites.") (emphasis added).
27   [154] James Hercher, *The IAB Finalizes CCPA Framework As Industry Readies For More
     Regulators*, ad exchanger (Dec. 5, 2019, 1:04 PM), https://www.adexchanger.com/online-
28   advertising/the-iab-finalizes-ccpa-framework-as-industry-readies-for-more-regulators/
     [https://perma.cc/Q2CX-GLU4].

SECOND AMENDED CLASS ACTION COMPLAINT
                                            CASE NO. 3:22-CV-04792-RS

1   117.   As a data broker, Oracle effectuates ongoing, comprehensive surveillance of the

2 Plaintiffs and Class members which grievously intrudes upon their privacy and which inevitably

3 results in the corrosion of their individual autonomy and the collective autonomy of the society at

4 large. Ordinary people, such as the Class members, do not and cannot possess an appropriate level

5 of knowledge about the substantial threats that Oracle's surveillance poses to their own autonomy

6 (in addition to lacking information sufficient to comprehend the nature and extent of Oracle's

7 surveillance and its other implications). The social harms posed by Oracle's conduct impair not

8 only individual autonomy, but the collective autonomy of Class members, as all members of a

9 society have an interest in the enforcement of privacy rights, freedom from surveillance, and

10 preservation of autonomy. Evisceration of these privacy values inexorably leads to the abrogation

11 of the autonomy and freedom of the citizenry which are essential to the proper functioning of

12 democratic republics. These harms caused by Oracle far outweigh the commercial benefits that

13 extend to a private corporation. In the context of Oracle's practices, valid consent from Plaintiffs

14 and the Class members is not only absent, it is not even possible.

15   118.   Plaintiffs and Class members in fact have not waived their fundamental right to be

16 free from the pervasive surveillance Oracle subjects them to. In any event, even were there any

17 basis to conclude that Plaintiffs and Class members could be considered to have waived their

18 reasonable expectation of privacy with respect to Oracle's practices (and there is not), such waiver

19 would be void and invalid as against public policy.

20   **F.   Oracle Knowingly and Intentionally Invaded Plaintiffs' and Class Members'
          Privacy.**

21

22   119.   On information and belief, Oracle was aware that its conduct of profiling Class

    members was tortious, and intended to violate Class members' privacy and other rights.

23

24   120.   Oracle CEO Larry Ellison has cynically and dismissively stated publicly that

25 privacy is "an illusion." As early as 2001, Ellison "call[ed] for the creation of a national ID

    system, even offering to donate the software to make it possible," for the purposes of facilitating

26

27

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                        CASE NO. 3:22-CV-04792-RS

1   intrusive and comprehensive government surveillance.[155] Ellison further stated, "[t]he privacy

2   you're concerned about is largely an illusion. All you have to give up is your illusions, not any of

3   your privacy. Right now, you can go onto the Internet and get a credit report about your neighbor

4   and find out where your neighbor works and how much they earn."[156]

5   121.   Oracle, at Ellison's direction, eventually effectuated the equivalent of a "national

6   ID system" owned and operated by Oracle, albeit one operating surreptitiously and without U.S.

7   citizens' knowledge or consent. Oracle proudly proclaims that the "Oracle ID Graph covers nearly

8   all U.S. adults through both owned and operated, and licensed data. It includes more than 220

9   million people [in the United States] over 18 years old and 115 million households . . . Starting

10   with [households] and the names and postal addresses of those households, the ID Graph was

11   expanded by adding online data such as cookies and email addresses as retailers took their

12   businesses online."[157]

13   122.   In 2016, Ellison, in describing Oracle's amassing of profiles on Class members

14   through its ID Graph, flippantly acknowledged that Oracle's profile-building conduct was privacy-

15   invasive, potentially illegal, and was "scaring the lawyers": "[Oracle's conduct] is a combination

16   of real-time looking at all of their social activity, real-time looking at where they are, including,

17   micro-locations – *this is scaring the lawyers who are shaking their heads and putting their hands*

18   *over their eyes* – knowing how much time you spend in a specific aisle of a specific store and what

19   is in that aisle of a store."[158]

20   123.   As noted above, Oracle has itself acknowledged the highly "invasive and

21   revealing"[159] nature of its own profile-building conduct, albeit indirectly. Without a trace of irony,

22   ───────────────────────

     [155]Jane Black, *Don't Make Privacy the Next Victim of Terror*, Bloomberg (Oct. 3, 2001),
23   https://www.bloomberg.com/news/articles/2001-10-03/dont-make-privacy-the-next-victim-of-
     terror [https://perma.cc/RC5M-D9PD].
24   [156] *Id.*

     [157] *About Moat Reach*, Oracle, https://docs.oracle.com/en/cloud/saas/data-cloud-moat-
25   reach/about_moat_reach/about_moat_reach.html [https://perma.cc/3CV4-AY2T].

26   [158] *See* TechEvents, *Openworld 2016 keynote by Larry Ellison: Complete, Integrated Cloud*,
     YouTube (Sept. 19, 2016), at 1:15:25-50, https://www.youtube.com/watch?v=WY5qhLwIqBA
27   (emphasis added).

     [159] *Oracle Corporation Submission to the Digital Platforms Inquiry*, Oracle (Mar. 1, 2019),
28   https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF

                                                                    SECOND AMENDED CLASS ACTION COMPLAINT
                              - 54 -   CASE NO. 3:22-CV-04792-RS

1   Oracle has argued to legislators both in the U.S. and internationally that its business rival Google

2   wrongfully builds "shadow profiles," "using massive amounts of consumer data, not all of which it

3   discloses to consumers, to micro-targe[t] advertising" to consumers without their consent.

4   However, Oracle's description of Google's conduct is virtually a word-for-word description of its

5   own conduct as a data broker. According to Oracle, Google's "shadow profiles" are:

> [M]assive, largely hidden datasets of online and offline activities. This information
> is collected through an extensive web of Google [*cf.* Oracle] services, which is
> difficult, if not impossible to avoid. *It is largely collected invisibly and without
> consumer consent.* [*cf. e.g.*, paragraph 101,[160] *supra*] by algorithms and artificial
> intelligence, this data reveals an intimate picture of a specific consumer's
> movements, socio-economics, demographics, "likes," activities and more. [*cf. e.g.*,
> paragraphs 60-71,[161] *supra*].[162]

10   124.   Oracle further states that Google's conduct—which precisely mirrors Oracle's own

11   as alleged in this Complaint—"works to provide *everything but privacy* for the consumer":

> Google [*cf.* Oracle] generates the majority of its revenue through advertising,
> powered by its ability to generate and combine large amounts of specific consumer
> data about consumer behavior on the internet with real time consumer activity and
> location data from mobile phones [*cf. e.g.*, paragraphs 41-59,[163] *supra*], as well as
> a myriad of other surreptitious collection points, such as internet cookies and
> application metadata. Google [*cf.* Oracle] uses the location data it collects from
> mobile devices over time to establish patterns of life for consumers and
> acknowledges tracking both signed in and signed out consumers to infer interest in
> a location and inform a profile for the purposes of selling ads [*cf. e.g.*, paragraph
> 69,[164] *supra*].[165]

[https://perma.cc/LHE4-B47C].

[160] Stating in relevant part: "Oracle sits atop a complex data collection and processing apparatus feeding its labyrinthine multinational data marketplace, making it impossible for ordinary persons to reasonably understand the true purpose and extent of Oracle's data collection, compiling of digital dossiers, and other data exploitation practices, which are opaque, if not invisible, to ordinary data subjects."

[161] Describing Oracle's aggregation and analysis of Class members' data to create intimate portraits of their activities.

[162] *Oracle Corporation Submission to the Digital Platforms Inquiry*, Oracle (Mar. 1, 2019), https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF [https://perma.cc/LHE4-B47C].

[163] Describing Oracle's use of cookies, pixels, JavaScript, and other means to surreptitiously collect data from Class members and combining that with offline purchase and location information.

[164] Oracle CEO Larry Ellison stated: "By collecting this data and marrying it to things like micro location information, Internet users' search histories, websites visits and product comparisons along with their demographic data, and past purchase data, Oracle will be able to predict purchase intent better than anyone."

[165] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

125.   Oracle has even publically undermined the supposedly exculpatory positions it has

taken in this litigation with respect to its own wiretapping conduct—but only when its rival

Google has taken those positions. In this litigation, Oracle argued that it could not be liable for

violation of the ECPA because it is a "party" to the communications between Plaintiffs and

websites.[166] But in a 2021 public-facing blog post on Oracle's website, an Oracle Executive Vice

President—clearly writing on behalf of Oracle—characterized an identical argument made by

Google as "ridiculous":

> When I call my dad using Verizon, I assume my dad and I are the only people in
> the conversation. The two of us are the first parties. I did not call my dad and
> Verizon; there aren't three of us on the call. But under Google's rules, Verizon is
> a first party to the call, and they should be able to advertise to us based on the
> restaurants or movies—or health or financial issues—we discussed on our call.
>
> So let's follow the phone call analogy to the web. Let's say I sit down and "call"
> the New York Times using my Chrome web browser—HTTP instead of my
> phone. Here, the consumer considers the New York Times a first party—just like
> when I call my dad. The New York Times also considers the consumer its first
> party (i.e. customer*). It's ridiculous to consider Google a first party to this
> interaction just because I am using Chrome, even if the New York Times hires
> Google to place ads or track analytics on its website.*[167]

126.   At least until August 2022, Oracle's bk.coretag.js JavaScript code was in fact on the

New York Times website, and Oracle thereby intercepted the contents of Plaintiffs'

communications with that website. *See* paragraph 6, *supra*. Oracle thus well understood that its

conduct was invasive and illegal, but pivoted to exculpatory arguments it had previously

characterized as "ridiculous" when it found it legally expedient (but ultimately fruitless[168]) to do

so.

127.   Oracle has further acknowledged that aspects of its profiling and targeting

conduct—which is augmented and informed via the use of the communications which Oracle

intercepts, as described herein—are potentially harmful to Class members, and are even "close to

enabling alcoholics." For example, in November of 2019, a news article, apparently quoting

---

[166] *See* Dkt. No. 23 at 19.

[167] Ken Glueck, *Google's Privacy Sandbox – We're all FLoCed,* Oracle Blog (Mar. 7, 2021),
https://www.oracle.com/news/announcement/blog/google-privacy-sandbox-030721/ (emphasis
added) [https://perma.cc/GMR7-DHHX].

[168] The Court rejected Oracle's "party exception" defense to the ECPA and CIPA claims. Dkt.
No. 49 at 14-15.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 sources within Oracle, stated that Oracle intended to "discontinue alcohol-based targeting."[169]

2 This was because Oracle appears to have recognized that "[v]ia Datalogix, companies could target

3 people who frequently bought alcohol – *which felt too close to enabling alcoholics*."[170] Yet as late

4 as July 2022—three years after it purported to cease this conduct, and only days before the

5 Complaint in this action was filed—Oracle continued to tout its ability to target "Alcohol

6 Beverage purchase based modeled audiences," including micro-targeting categories tracking

7 people's alcohol use habits, such as "Malt Beverage Buyers" or "Wine or Liquor Store Top

8 Spenders."[171] Oracle thus continues to knowingly engage in profiling and targeting conduct as

9 described herein that it is aware is harmful and pernicious. Plaintiffs' investigation of this conduct

10 is ongoing, however, based on information and belief, Oracle's alcohol-based targeting is

11 effectuated through profiling and micro-targeting informed in part by communications intercepted

12 through the bk.coretag.js JavaScript interception mechanism.

13   128.   Oracle has stated in both its privacy policies[172] and in this litigation that Oracle

14 does "not use any data it receives from customers to create sensitive interest segments," including

15 those related to "political" orientation, "and prohibits its customers from doing the same;" as

16 such, "Consumers are not and cannot be harmed by Oracle's practices[.]"[173] But this statement is

17 false—Oracle has (or has had during the class period) *entire product lines* devoted precisely to

---

[169] Sarah Sluis, *Oracle Data Cloud Cuts Staff As It Tries To Move Beyond Third-Party Data*, ad exchanger (Sept. 24, 2019, 6:45 PM) https://www.adexchanger.com/platforms/oracle-data-cloud-cuts-staff-as-it-tries-to-move-beyond-third-party-data/ [https://perma.cc/R4WK-6HNW].

[170] *Id.* (emphasis added).

[171] *Alcohol and Beverage Digital Audiences and Contextual Segments*, Oracle, https://www.oracle.com/middleeast/a/ocom/docs/beverage-digital-audiences-contextual-segments.pdf [https://perma.cc/YEL7-DKG6]. The metadata for this document states it was created on July 12, 2022, and according to archive.org, the earliest this document was made publicly available on Oracle's website was August 17, 2022. *See* https://web.archive.org/web/20220601000000*/https://www.oracle.com/middleeast/a/ocom/docs/beverage-digital-audiences-contextual-segments.pdf.

[172] As of the filing of this action in August 2022, the Oracle Advertising Privacy Policy stated that "Oracle does not create any online interest segments that reflect personal information that we consider sensitive . . . we treat the following types of personal information as sensitive: . . . certain aspects linked to personal life, such as religious, *political*, or sexual orientation." *Oracle Advertising Privacy Policy*, Oracle (version updated May 5, 2022), https://www.oracle.com/legal/privacy/advertising-previous-privacy-policy-050522.html [https://perma.cc/MP25-TAXY] (emphasis added).

[173] Dkt. No. 63 at 3.

SECOND AMENDED CLASS ACTION COMPLAINT
                                                    CASE NO. 3:22-CV-04792-RS

1   selling such "sensitive interest segments" based on political orientation. Oracle's "DLX [short for

2   'Datalogix'] Politics gives you access to accurate political audiences built from leading sources of

3   voter registration data. It's your personal ballot box of real voters based on their party affiliation,

4   voting county/state, political views, financial donor history and voting behavior."[174] Through

5   DLX Politics, Oracle sells or sold interests segments based on, *inter alia*, "conservative,"

6   "progressive," or "independent" political orientations, inferred from data regarding at least

7   political donations.[175] On information and belief, Oracle has continued sell interest segments to

8   third parties based on political orientation despite its public statements in its privacy policies to the

9   contrary.

10   129.   Moreover, Oracle's "2019 Data Directory," showcasing the data that its "data

11   providers" sell through Oracle's Data Marketplace, includes at least a dozen separate vendors who

12   openly advertise the sale of detailed political information on Class members through Oracle's Data

13   Marketplace, which can be synchronized with the profiles Oracle maintains on "nearly all U.S.

14   adults" through its ID Graph.[176] On information and belief, the data Oracle intercepts through the

15   bk.coretag.js JavaScipt is associated with these preexisting user profiles.

16   130.   Recent reporting indicates that, despite Oracle's representations to the public,

17   Oracle has continued to offer "sensitive interest segments" for sale, including those based on

18   political orientation. In June of 2023, nonprofit news publication The Markup analyzed a database

19   of 650,000 "audience segments," which were "newly unearthed on the website of Microsoft's ad

20   platform Xandr."[177] The trove of data indicates that advertisers could also target people based on

21   sensitive information," including political orientation, through audience segments made available

22

23   [174] *The Audience Playbook, Inspiration for winning campaigns*, Oracle (Aug. 2016),
     http://online.pubhtml5.com/mdhz/hgpp/#p=64 [https://perma.cc/MRC2-RFVV].

24   [175] *Id.* at 65.

25   [176] *2019 Data Directory*, Oracle (2019),
     https://web.archive.org/web/20210405154410/https://www.oracle.com/us/solutions/cloud/data-

26   directory-2810741.pdf [https://perma.cc/EV8L-PG7V].

27   [177] Jon Keegan and Joel Eastwood, *From "Heavy Purchasers" of Pregnancy Tests to the
     Depression-Prone: We Found 650,000 Ways Advertisers Label You*, The Markup (June 8, 2023),
     https://themarkup.org/privacy/2023/06/08/from-heavy-purchasers-of-pregnancy-tests-to-the-

28   depression-prone-we-found-650000-ways-advertisers-label-you [https://perma.cc/MUG2-N38J].

SECOND AMENDED CLASS ACTION COMPLAINT
                                                                      CASE NO. 3:22-CV-04792-RS

by Oracle.[178] The database[179]—which the article makes searchable—demonstrates that Oracle

appears to continue (or at least continued as of May 2021) to offer political interest advertising

segments for sale,[180] including segments such as supporters of "Donald Trump," donors to

"Progressive Causes," backers of the "Tea Party," and an array of political labels like

"Conservative," "Liberal," "Independent," and "Undecided Voter."[181]

131.   Oracle's duplicitousness on this issue is not a product of happenstance or

misunderstanding—Oracle deliberately conceals from the public that it creates profiles of them

based on sensitive information such as their political orientations, and then further associates data

it surreptitiously intercepts when Class members communicate with websites with those profiles.

It deliberately conceals these facts because it knows the conduct it engages in is harmful and

invasive of Class members' privacy and would be immediately recognized as such once publicly

revealed.

---

[178] *Id.*

[179] The database described in The Markup article appears to have been made available through Xandr as an online excel spreadsheet. *See* Ingo Dachwitz, *The adtech industry tracks most of what you do on the Internet. This file shows just how much*, Netzpolitik.org (June 7, 2023), https://netzpolitik.org/2023/surveillance-advertising-in-europe-the-adtech-industry-tracks-most-of-what-you-do-on-the-internet-this-file-shows-just-how-much/ [https://perma.cc/TVB5-YNXF].

[180] A list of political interest segments available through Oracle, all of which are drawn from the database referenced in The Markup article, is attached as Exhibit C.

[181] Screenshot from The Markup article. Many of these segments were created by Oracle. As the screenshot indicates, the advertising segment "Tea Party (BlueKai)" is derived from Oracle's AddThis and is listed in the Xandr database as available through "Audiences by Oracle (BlueKai, Datalogix, AddThis)."

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   132.   As shown above, Oracle has engaged in artifice and misinformation as tools of

2   coercion deployed intentionally to create unwitting participants in its surveillance scheme as

3   described herein. Oracle knows Class members cannot and do not consent to its privacy-invasive

4   profiling and targeting activities. Yet Oracle has knowingly and deliberately continued to engage

5   in conduct that it has publicly acknowledged is highly invasive and harmful—in a word, tortious.

6   As described above, on information and belief, Oracle has been aware of the tortious and illegal

7   nature of its conduct since at least 2016; it is not the case that Oracle engaged in this conduct only

8   under the "mere possibility Oracle's data collection activities could at some future date be deemed

9   tortious."[182]

10   133.   Plaintiffs' investigation into Oracle's understanding of the tortious nature of its

11   conduct is ongoing. Plaintiffs have requested any internal Oracle communications referring to the

12   company's relevant privacy practices as problematic, but have not yet received such discovery.

13   On information and belief, Oracle employees are and were aware that Oracle's privacy practices

14   are highly problematic. For example, on June 19, 2020, on the website news.ycombinator.com,

15   run by the well-known tech startup "incubator" Y Combinator,[183] an anonymous former Oracle

16   employee posted the following: "I worked at oracle on the bluekai product (search 'oracle' in my

17   comment history). I helped deliver data using bluekai from oracle to platforms like facebook and

18   google. AMA. ["ask me anything"]."[184] In response to a post stating "If you want to check out

19   what bluekai knows about your browser: https://datacloudoptout.oracle.com/registry/," the former

20   Oracle employee stated the following: "It should be known that this tool [i.e., Oracle's data opt-out

21   tool] is purposefully never updated and knowingly inaccurate."[185] Thus, a former Oracle

22

---

[182] Dkt. No. 77 at 11, fn. 11.

23   [183] *See Y Combinator*, Wikipedia, https://en.wikipedia.org/wiki/Y_Combinator
[https://perma.cc/VM4F-RJYP] ("Y Combinator Management, LLC (YC) is an American

24   technology startup accelerator launched in March 2005 which has been used to launch more than
4,000 companies . . . Companies started via Y Combinator include Airbnb, Coinbase, Cruise,

25   DoorDash, Dropbox, Instacart, Reddit, Stripe, and Twitch.").

26   [184] soared, Comment to Oracle's BlueKai tracks people across the web – that data spilled online
(techcrunh.com), Hacker News (June 19, 2020),

27   https://news.ycombinator.com/item?id=23575517#23575760 [https://perma.cc/L9Y3-WRFH].

28   [185] soared, Comment to Oracle's BlueKai tracks people across the web – that data spilled online
(techcrunh.com), Hacker News (June 19, 2020),

SECOND AMENDED CLASS ACTION COMPLAINT
                                            CASE NO. 3:22-CV-04792-RS

1   employee has stated publicly that Oracle's opt-out tool—which Oracle has touted in this litigation

2   as evidence of its privacy-protective practices[186]—was *intentionally* "never updated and

3   knowingly inaccurate"—in other words, a farce. Oracle employees were therefore well aware not

4   only that the company's privacy practices were problematic, but that Oracle intentionally and

5   deliberately frustrated Class members' ability—statutorily prescribed by the CCPA[187]—to opt out

6   of its tracking and profiling practices. Oracle thus deliberately and intentionally invaded Class

7   members' privacy, and then frustrated their ability to stop it from doing so.

8   **VII.**   **CLASS ALLEGATIONS**

9   134.   Plaintiffs bring this class action, pursuant to Rule 23 of the Federal Rules of Civil

10   Procedure, individually and on behalf of all members of the following classes, which are jointly

11   referred to throughout this Complaint as the "Classes:"

12   California Class:

13
     All natural persons located in California whose personal information, or data
     derived from their personal information, was used to create a profile and made
14   available for sale or use through Oracle's ID Graph or Data Marketplace.

15   California Invasion of Privacy Act ("CIPA") Sub-Class:

16
     All members of the California Class whose contents of their electronic
     communications were intercepted by the use of Oracle's bk-coretag.js
17   functionality.

18   Florida Class:

19
     All natural persons located in Florida whose personal information, or data derived
     from their personal information, was used to create a profile and made available
20   for sale or use through Oracle's ID Graph or Data Marketplace.

21   Florida Security of Communications Act ("FSCA") Sub-Class:

22
     All members of the Florida Class whose contents of their electronic
     communications were intercepted by the use of Oracle's bk-coretag.js
23   functionality.

24   ─────────────────
https://news.ycombinator.com/item?id=23575517#23577506 [https://perma.cc/L9Y3-WRFH].

25   [186] *See, e.g.,* Dkt. No. 63 at 1-2 (complaining that "Plaintiffs ignore that Oracle is lawfully
operating within laws designed to protect California consumers . . . [they] ignore that internet

26   users *are given the choice to opt out of the alleged data collection practices*." (emphasis added));
Dkt. No. 70 at 13 (attempting to distinguish Oracle's conduct from that of other privacy-invasive

27   data aggregators on the grounds that "Oracle readily and broadly allows opt-outs").

28   [187] *See* Cal Civ. Code § 1798.110 (requiring Oracle to disclose to consumers the "specific pieces
of personal information it has collected about that consumer."); § 1798.120 (providing the "Right
to Opt Out of Sale or Sharing of Personal Information").

   SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   Electronic Communications Privacy Act ("ECPA") Class:

2   All natural persons located in the United States whose personal information, or
     data derived from their personal information, was used to create a profile and
3   made available for sale or use through Oracle's ID Graph or Data Marketplace,
     and whose contents of their electronic communications were intercepted by the use
4   of Oracle's bk-coretag.js functionality.

5   135.   Excluded from the Classes are the following individuals: officers and directors of

6   Oracle and its parents, subsidiaries, affiliates, and any entity in which Oracle has a controlling

7   interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate

8   family members.

9   136.   Plaintiffs reserve the right to modify or amend the definition of each of the

10   proposed Classes before the Court determines whether certification is appropriate.

11   137.   This action readily satisfies the requirements set forth under Federal Rule of Civil

12   Procedure 23:

13   a.   Each Class is so numerous that joinder of all members is impracticable.

14   Upon information and belief, Class members number in the millions.

15   b.   There are questions of law or fact common to the Classes. These questions

16   include, but are not limited to, the following:

17   1)   Whether Oracle's acts and practices complained of herein amount

18   to egregious breaches of social norms;

19   2)   Whether Oracle acted intentionally in violating Plaintiffs' and Class

20   members' privacy rights;

21   3)   Whether Oracle was unjustly enriched as a result of its violations of

22   Plaintiffs' and Class members' privacy rights;

23   4)   Whether an injunction should issue; and

24   5)   Whether declaratory relief should be granted.

25   c.   Plaintiffs' claims are typical of the claims of the Classes. Plaintiffs and the

26   Class members did not consent to Oracle's interception, collection, analysis, and sale or their

27   personal information, which acts form the basis for this suit.

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

1   d.   Moreover, like all Class members, Plaintiffs suffer a substantial risk of

2 repeated injury in the future. Each Plaintiff continues to use devices that are capable of reporting

3 personal information to Oracle. Oracle's actions have thwarted and continue to threaten

4 Plaintiffs' (and Class members') ability to exercise control over their own privacy while using

5 their devices. Because the conduct complained of herein is systemic, Plaintiffs and all Class

6 members face substantial risk of the same injury in the future. Oracle's conduct is common to all

7 Class members and represents a common pattern of conduct resulting in injury to all members of

8 the Classes. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any

9 other Class member.

10   e.   Plaintiffs will fairly and adequately protect the interests of the Classes.

11 Plaintiffs' interests do not conflict with the interests of the Class members. Furthermore,

12 Plaintiffs have retained competent counsel experienced in class action litigation, consumer

13 protection litigation, and electronic privacy litigation. Plaintiffs' counsel will fairly and

14 adequately protect and represent the interests of the Classes. Federal Rule of Civil Procedure

15 23(a)(4) and 23(g) are satisfied.

16   f.   In acting as above-alleged, Oracle has acted on grounds generally

17 applicable to the Classes, thereby making final injunctive relief and corresponding declaratory

18 relief each appropriate with respect to the Classes as a whole. The prosecution of separate actions

19 by individual Class members would create the risk of inconsistent or varying adjudications with

20 respect to individual Class members that would establish incompatible standards of conduct for

21 Oracle.

22 **VIII.   CAUSES OF ACTION**

23
<div align="center">

First Cause of Action
Invasion of Privacy Under the California Constitution
(on behalf of the California Class)
</div>

24

25   138.   Plaintiff Katz-Lacabe and the California Class members repeat and reallege all

26 preceding paragraphs contained herein.

27   139.   Article I, section 1 of the California Constitution provides: "All people are by

28 nature free and independent and have inalienable rights. Among these are enjoying and defending

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety,

2   happiness, *and privacy*." The phrase "*and privacy*" was added by the "Privacy Initiative" adopted

3   by California voters in 1972.

4   140.   The phrase "and privacy" was added in 1972 after voters approved a proposed

5   legislative constitutional amendment designated as Proposition 11. Proposition 11 was intended to

6   curb businesses' control over the unauthorized collection and use of peoples' personal

7   information, as the ballot argument stated:

8   The right of privacy is the right to be left alone…It prevents government and
        business interests from collecting and stockpiling unnecessary information about
9   us and from misusing information gathered for one purpose in order to serve other
        purposes or to embarrass us. Fundamental to our privacy is the ability to control
10   circulation of personal information. This is essential to social relationships and
        personal freedom.[188]

11   141.   This amended constitutional provision addresses the concern over accelerating

12   encroachment on personal freedom and security caused by increasing surveillance and data

13   collection activity in contemporary society. Its proponents meant to afford individuals more

14   measure of protection against this most modern threat to personal privacy:

15
        Computerization of records makes it possible to create 'cradle-to-grave' profiles of
16   every American. At present there are no effective restraints on the information
        activities of government and business. This amendment creates a legal and
17   enforceable right of privacy for every Californian.[189]

18   In recognizing these privacy rights, the California Constitution provides insight into and serves to

19   define the nature of the reasonable expectation of privacy of an objectively reasonable California

20   resident. In contravention to the California Constitution and the reasonable expectations of

21   privacy of California residents, Oracle "stockpil[es] unnecessary information about [California

22   Class members] and [] misus[es]information gathered for one purpose in order to serve other

23   purposes," creating "cradle-to-grave" profiles of California Class members.

24   142.   Plaintiff Katz-Lacabe and the California Class members maintain a reasonable

25   expectation of privacy in the conduct of their lives, including their internet browsing activities and

26   in their electronic communications and exchange of personal data. The reality of modern life

27
     [188] Ballot Pamp., Proposed Stats. & Amends. To Cal. Const. With Arguments to Voters. Gen.
28   Election *26 (Nov. 7, 1972).
     [189] *Id.*

1   increasingly requires that much of our daily activities are conducted online—Plaintiff Katz-Lacabe

2   and the California Class members have no practical choice or ability but to conduct their daily

3   lives substantially in the digital world, connected to the Internet. The necessary engagement with

4   the digital world makes Plaintiff Katz-Lacabe's and the California Class members' private lives

5   susceptible to unlawful observation and recording, capable of yielding a comprehensive and

6   intrusive chronicle of Plaintiff Katz-Lacabe's and the California Class members' lives. If Plaintiff

7   Katz-Lacabe and the California Class members do not have a reasonable expectation of privacy in

8   the conduct of their lives online and the digital transmission of their personal data, they can have

9   no reasonable expectation of privacy for virtually any facet of their lives.

10   143.   Oracle, in violation of Plaintiff Katz-Lacabe's and the California Class members'

11   reasonable expectation of privacy, intercepts, collects, tracks and compiles their web browsing

12   activity and communications.

13   144.   The nature and volume of the web browsing data collected is such that Oracle's

14   practice of compiling dossiers based on the data it collects violates Plaintiff Katz-Lacabe's and the

15   California Class members' reasonable expectation of privacy. Technological advances, such as

16   Oracle's use of cookies, pixels, JavaScript, and other means to track and compile internet

17   browsing activity, electronic purchases, and electronic communications, provide Oracle with the

18   means to assemble a comprehensive chronicle of Plaintiff Katz-Lacabe's and the California Class

19   members' lives heretofore unseen. Oracle collects and compiles personal information such as

20   Plaintiff Katz-Lacabe's and the California Class members' email addresses, location data, and web

21   browsing information, including that relating to race, religion, sexual orientation, and health. Such

22   information is "personal information" under California law, which defines personal information as

23   including "Internet or other electronic network activity information," such as "browsing history,

24   search history, and information regarding a consumer's interaction with an internet website,

25   application, or advertisement." Cal. Civ. Code § 1798.140.

26   145.   Oracle also collects and analyzes Plaintiff Katz-Lacabe's and the California Class

27   members' real-world offline activity, including activities like brick-and-mortar store purchases and

28   location information, and compiles computerized records of those activities. Plaintiff Katz-Lacabe

1   and the California Class members do not and cannot know which specific real-world offline

2   activities Oracle may or may not be collecting and analyzing and adding to the digital dossiers it

3   compiles on them.

4   146.   Oracle's conduct as described herein is highly offensive to a reasonable person and

5   constitutes an egregious breach of social norms, specifically including the following:

6   a.   Oracle engages in dragnet-style collection and interception of Plaintiff

7   Katz-Lacabe's and the California Class members Internet activity, including their

8   communications with websites, thereby learning intimate details of their daily lives based on the

9   massive amount of information collected about them.

10   b.   Oracle also collects minute details about Plaintiff Katz-Lacabe's and the

11 California Class members' *offline* activities, including their brick-and-mortar purchases and

12 location information. By its very nature, Plaintiff Katz-Lacabe and the California Class members

13 cannot be aware of or consent to this conduct.

14   c.   Oracle creates dossiers based on this online and offline data, which

15 constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California

16 Constitution was created to constrain.

17   147.   Oracle's amassing of the electronic information reflecting all aspects of Plaintiff

18 Katz-Lacabe's and the California Class members' lives into dossiers for future or present use is in

19 and of itself a violation of Plaintiff Katz-Lacabe's and the California Class members' right to

20 privacy in light of the serious risk these dossiers pose to their autonomy. Additionally, those

21 dossiers are and can be used to further invade Plaintiffs' privacy, by, inter alia, allowing third

22 parties to learn intimate details of Plaintiff Katz-Lacabe's and the California Class members' lives,

23 and target them for advertising, political, and other purposes, as described herein, thereby harming

24 them through the abrogation of their autonomy and their ability to control dissemination and use of

25 information about them. Additionally, as described above, the social harms posed by Oracle's

26 conduct impair not only individual autonomy, but the collective autonomy of California Class

27 members, which autonomy is essential to the proper functioning of democratic republics.

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                                       CASE NO. 3:22-CV-04792-RS

1   148.   Plaintiffs have been harmed by Oracle's indiscriminate collection and sale of their

2   internet activity, their geolocation information, and their real world activities and purchases.

3   149.   Privacy advocates have repeatedly decried Oracle's practices. Oracle's conduct

4   described herein has been the subject of numerous legal complaints and lawsuits in Europe and the

5   U.K. by privacy advocates.

6   150.   Legislators have recognized the pernicious and privacy-invasive nature of Oracle's

7   conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau

8   to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to

9   sell [consumers'] personal information without any legal protections" and that selling consumers'

10 personal information "giving them no choice in the matter, is an egregious abuse of consumers'

11 privacy." Senators Warren and Wyden have also stated that "[d]ata brokers profit from the

12 location data of millions of people, posing serious risks to Americans everywhere by selling their

13 most private information." The FTC has also warned consumers about the "shadowy" "data

14 broker ecosystem" where "companies have a profit motive to share data at an unprecedented scale

15 and granularity," including a "staggering" amount of "highly personal information that people

16 choose not to disclose even to family, friends, or colleagues."[190]

17   151.   Oracle has violated Plaintiff Katz-Lacabe's and the California Class members'

18 reasonable expectation of privacy via Oracle's review, analysis, dissemination, and subsequent

19 uses of Plaintiffs' and California Class members' private and other browsing activity through

20 Oracle's Data Cloud, ID Graph and Data Marketplace.

21   152.   Oracle's practices as alleged herein violate Plaintiff Katz-Lacabe's and the

22 California Class members' reasonable expectation of privacy and are highly offensive to a

23 reasonable person, and constitute an egregious breach of the social norms.

24   153.   The right to privacy in California's constitution creates a right of action for

25 California residents against private entities such as Oracle. Oracle lacks a legitimate business

26 _____

27 [190] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data,* The Federal Trade Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-

28 health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   interest in stockpiling and compiling the personal information of Plaintiff Katz-Lacabe and the

2   California Class members.

3   154.   Plaintiff Katz-Lacabe and the California Class members have been damaged by

4   Oracle's invasion of their privacy and are entitled to just compensation and injunctive relief.

5   **Second Cause of Action**
                    Intrusion Upon Seclusion Under California Common Law
6   **(on behalf of the California Class)**

7   155.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

8   156.   Plaintiffs allege intrusion upon seclusion under California law on behalf of the

9   California Class.

10   157.   Plaintiffs asserting claims for intrusion upon seclusion must plead (1) intrusion into

11   a private place, conversation, or matter; (2) in a manner highly offensive to a reasonable person.

12   158.   Plaintiffs and California Class members maintain a reasonable expectation of

13   privacy in the conduct of their lives, including their Internet browsing activities and in their

14   electronic communications and exchange of personal data. The reality of modern life increasingly

15   requires that much of our daily activities are conducted online—Plaintiffs and California Class

16   members have no practical choice or ability but to conduct their daily lives substantially in the

17   digital world, connected to the Internet. The necessary engagement with the digital world makes

18   Plaintiffs' and California Class members' private lives susceptible to unlawful observation and

19   recording that is capable of yielding an comprehensive and intrusive chronicle of Plaintiffs' and

20   California Class members' lives. If Plaintiffs and California Class members do not have

21   reasonable expectation of privacy in the conduct of their lives online and the digital transmission

22   of their personal data, they can have no reasonable expectation of privacy for virtually any facet of

23   their lives.

24   159.   Oracle, in violation of Plaintiffs' and California Class members' reasonable

25   expectation of privacy, intercepts, collects, tracks, and compiles their web browsing activity and

26   communications.

27   160.   The nature and volume of the web browsing data collected is such that Oracle's

28   practice of compiling dossiers based on the data it collects violates Plaintiffs' and California Class

1 members' reasonable expectation of privacy. Technological advances, such as Oracle's use of

2 cookies, pixels, and other means to track and compile internet browsing activity, electronic

3 purchases, and electronic communications, provide Oracle with the means to assemble a

4 comprehensive chronicle of Plaintiffs' and California Class members' lives heretofore unseen.

5 Oracle collects and compiles personal information such as Plaintiffs' and California Class

6 members' email addresses, location data, and web browsing information, including that relating to

7 race, religion, sexual orientation, and health. Such information is "personal information" under

8 California law which defines personal information as including "Internet or other electronic

9 network activity information," such as "browsing history, search history, and information

10 regarding a consumer's interaction with an internet website, application, or advertisement." Cal.

11 Civ. Code § 1798.140.

12   161.   Oracle also collects and analyzes Plaintiffs' and California Class members' real-

13 world offline activity, including activities like brick-and-mortar store purchases and location

14 information, and compiles computerized records of those activities. Plaintiffs and California Class

15 members do not and cannot know which specific real-world offline activities Oracle may or may

16 not be collecting and analyzing and adding to the digital dossiers it compiles on them.

17   162.   Oracle's conduct as described herein is highly offensive to a reasonable person and

18 constitutes an egregious breach of social norms, specifically including the following:

19   a.   Oracle engages in dragnet-style collection and interception of Plaintiffs'

20 and California Class members' Internet activity, including their communications with websites,

21 thereby learning intimate details of their daily lives based on the massive amount of information

22 collected about them.

23   b.   Oracle also collects minute details about Plaintiffs' and California Class

24 members' *offline* activities, including their brick-and-mortar purchases and location information.

25 By its very nature, Plaintiffs and California Class members cannot be aware of or consent to this

26 conduct.

27

28

1   c.   Oracle creates dossiers based on this online and offline data, which

2 constitute precisely the sort of "cradle-to-grave profiles" the right to privacy under the California

3 Constitution was created to constrain.

4   163.   Oracle's amassing of the electronic information reflecting all aspects of Plaintiffs'

5 and California Class members' lives into dossiers for future or present use is in and of itself a

6 violation of Plaintiffs' and California Class members' right to privacy in light of the serious risk

7 these dossiers pose to their autonomy. Additionally, those dossiers are and can be used to further

8 invade Plaintiffs' and California Class members' privacy, by, inter alia, allowing third parties to

9 learn intimate details of Plaintiffs' and California Class members' lives, and target them for

10 advertising, political, and other purposes, as described herein, thereby harming them through the

11 abrogation of their autonomy and their ability to control the dissemination and use of information

12 about them. Additionally, as described above, the social harms posed by Oracle's conduct impair

13 not only individual autonomy, but the collective autonomy of California Class members, which

14 autonomy is essential to the proper functioning of democratic republics.

15   164.   Privacy advocates have repeatedly decried Oracle's practices. Oracle's conduct

16 described herein has been the subject of numerous legal complaints and lawsuits in Europe and the

17 U.K. by privacy advocates. For example, at least until September 2020, Oracle tracked and

18 compiled information on Internet users in the European Union and the United Kingdom using data

19 derived from "third-parties," as described in detail above.[191] As noted in the press, Oracle's

20 announcement that it would no longer make this functionality available in Europe and the U.K.

21 came "just weeks after Oracle and rival data broker Salesforce were named in a class-action

22 lawsuit in both the U.K. and the Netherlands that could result in the two companies having to pay

23 up to $11.7 billion in fines under GDPR rules."[192] Oracle publicly described that lawsuit as a

24

25

---

26 [191] Ronan Shields, *Oracle to Shutter Third-Party Data Services in Europe*, Adweek (Sept. 9,
27 2020), https://www.adweek.com/programmatic/oracle-to-shutter-third-party-data-services-in-europe/ [https://perma.cc/6VAK-2G5U].
28 [192] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   "shake-down"—yet it purported to cease certain of the practices complained of in that lawsuit only

2   weeks after it was filed.[193]

3   165.   Legislators have recognized the pernicious and privacy-invasive nature of Oracle's

4   conduct as described herein. Senator Wyden, in urging the Consumer Financial Protection Bureau

5   to take action against data brokers, stated that "[d]ata brokers are serving as shady middlemen to

6   sell [consumers'] personal information without any legal protections" and that selling consumers'

7   personal information and "giving them no choice in the matter, is an egregious abuse of

8   consumers' privacy." Senators Warren and Wyden have also stated that "[d]ata brokers profit

9   from the location data of millions of people, posing serious risks to Americans everywhere by

10   selling their most private information." The FTC has also warned consumers about the "shadowy"

11   "data broker ecosystem" where "companies have a profit motive to share data at an unprecedented

12   scale and granularity," including a "staggering" amount of "highly personal information that

13   people choose not to disclose even to family, friends, or colleagues."[194]

14   166.   Oracle has violated Plaintiffs' and California Class members' reasonable

15   expectation of privacy via Oracle's review, analysis, dissemination and subsequent uses of

16   Plaintiffs' and California Class members' private and other browsing activity through Oracle's

17   Data Cloud, ID Graph, and Data Marketplace.

18   167.   Oracle's practices as alleged herein violate Plaintiffs' and California Class

19   members' reasonable expectation of privacy and are highly offensive to a reasonable person, and

20   constitute an egregious breach of the social norms.

21   168.   Oracle lacks a legitimate business interest in stockpiling and compiling the personal

22   information of Plaintiffs and California Class members.

23

24   _____

25   [193] Natasha Lomas, *Oracle and Salesforce Hit with GDPR Class Action Lawsuits Over Cookie Tracking Consent*, TechCrunch (Aug. 14, 2020), https://techcrunch.com/2020/08/14/oracle-and-salesforce-hit-with-gdpr-class-action-lawsuits-over-cookie-tracking-consent/

26   [https://perma.cc/79R7-SFU9].

27   [194] Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the law Against Illegal Use and Sharing of Highly Sensitive Data,* The Federal Trade Commission (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-

28   health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use [https://perma.cc/V6XT-85YX].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   169.   Plaintiffs and California Class members have been damaged by Oracle's invasion

2   of their privacy and are entitled to just compensation and injunctive relief.

3   170.   As a result of Oracle's actions, Plaintiffs and California Class members seek

4   injunctive relief, in the form of Oracle's cessation of tracking practices in violation of Plaintiffs

5   and California Class members' rights, and destruction of all personal data obtained in violation of

6   Plaintiffs and California Class members' rights.

7   171.   As a result of Oracle's actions, Plaintiffs and California Class members seek

8   nominal and punitive damages in an amount to be determined at trial. Plaintiffs and California

9   Class members seek punitive damages because Oracle's actions—which were malicious,

10   oppressive, willful—were calculated to injure Plaintiffs and made in conscious disregard of

11   Plaintiffs' rights. Punitive damages are warranted to deter Oracle from engaging in future

12   misconduct.

13   172.   Plaintiffs seek restitution for the unjust enrichment obtained by Oracle as a result of

14   unlawfully collecting Plaintiffs' personal data. These intrusions are highly offensive to a

15   reasonable person. Further, the extent of the intrusion cannot be fully known, as the nature of

16   privacy invasion involves sharing Plaintiffs' and California Class members' personal information

17   with potentially countless third parties, known and unknown, for undisclosed and potentially

18   unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Oracle's

19   conduct is the fact that Oracle's principal goal is and was to surreptitiously monitor Plaintiffs and

20   California Class members and to allow third-parties to do the same.

21   173.   The threat posed by advancements in technology and the ability to create detailed

22   dossiers therefrom was recognized half a century ago. *See generally* Arthur R. Miller, *The Assault*

23   *on Privacy* 24–54 (1971). With monumental increases in technologies, Professor Miller's alarm 50

24   years ago about technology's assault on privacy has now taken on special urgency: precisely the

25   concerns he warned of have come to fruition in Oracle's conduct. Through this lawsuit Plaintiff

26   and California Class members seek to vindicate their common law right against Oracle's ongoing

27   assault on their privacy.

28

Third Cause of Action
Intrusion Upon Seclusion Under Florida Common Law
(on behalf of the Florida Class)

174.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

175.   Plaintiffs allege that Florida law on intrusion upon seclusion is applicable for all members of the Florida Class.

176.   Under Florida law, one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or her private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person. *See* Restatement (Second) of Torts § 652B (Am. Law Inst. 1977).

177.   Oracle's conduct electronically intrudes into Dr. Golbeck's home and computer by surveilling her internet browsing activity and communications with websites, as described above, which were conducted from the solitude of her own home and her computer.

178.   Dr. Golbeck has a reasonable expectation of privacy to be free from Oracle's pervasive surveillance of her in home. Florida courts recognize that that engaging in repeated surveillance of another person—via physical *or* electronic means—can constitute the tort of intrusion upon seclusion. Oracle's conduct in systematically surveilling Dr. Golbeck in her home by surveilling her browsing on her computer is tantamount to erecting a camera in her home as she browses the internet, in order to thereafter surveil and record her activities on a consistent basis.

179.   The Florida Supreme Court has explained that invasion of privacy by intrusion "is a tort in which the focus is the right of a private person to be free from public gaze." *Allstate Ins. Co. v. Ginsberg*, 863 So.2d 156, 162 (Fla. 2003). Given the volume and sensitivity of data on them, modern cell phones and laptop computers are generally kept "free from public gaze." Florida courts have specifically recognized that accessing a plaintiff's phone and its contents constitutes intrusion into a private "place." Florida Courts have also recognized an objectively reasonable expectation of privacy in one's computer. Florida courts further recognize a reasonable expectation of privacy in electronic spaces, such as email accounts, where access to the electronic space was generally kept private.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   180.   Dr. Golbeck's electronic devices constitute private places under Florida law. At all

2   times, Dr. Golbeck kept access to her devices, including her laptop and cell phone, and the

3   information therein, including her web browsing history and communications with websites taking

4   place therein, private. Dr. Golbeck's devices are and were password protected, and Dr. Golbeck

5   generally did not allow others to access any them. Oracle intruded into these electronic spaces by,

6   *inter alia*, intercepting the contents of her communications with websites and otherwise

7   systematically surveilling her activities on her devices.

8   181.   Florida courts have also recognized that noxious, offensive conduct that takes place

9   through remote electronic means, but that is directed at a plaintiff while that plaintiff is in her

10   home, supports a claim for intrusion upon seclusion under the common law. Much of Dr.

11   Golbeck's online activity takes and took place within her home, which Oracle deliberately

12   intruded into.

13   182.   Oracle openly touts its ability to surveil and manipulate Florida Class members

14   within the confines of their homes. Oracle states that the Oracle ID Graph is "comprised of 115M

15   households."[195] It further enables its clients to surveil and manipulate Florida Class members in

16   their homes by "[t]arget[ing] households within a specific radius."[196] Indeed, a central function of

17   the ID Graph is to surveil and target Florida Class members in their homes and link that activity to

18   the digital dossiers it compiles on them. Oracle states that "The Oracle BlueKai's ID Graph is a

19   critical piece of our 'portfolio approach,' . . . . The ID graph enables Oracle to reach 115 million

20   households in the US today, and after removing cookies and MAIDs, Oracle will still be able to

21   reach 99% of those households."[197] Oracle represents the ID Graph as linking "real people" in

22   their homes to the various other identifiers in its datasets.[198]

23

24

25   [195] *Activation Playbook*, Oracle (2020), https://www.oracle.com/za/a/ocom/docs/cx-activation-vertical-playbook-2020.pdf [https://perma.cc/TYS5-NKX4].

26   [196] *Id.*

27   [197] Brigitte Yuille, *3 Ways Oracle's Portfolio Approach Helps Advertisers Prepare for the Future of Identity*, Oracle Advertising Blog (May 18, 2021), https://blogs.oracle.com/advertising/post/3-ways-oracle%E2%80%99s-portfolio-approach-helps-advertisers-prepare-for-the-future-of-identity [https://perma.cc/EKB7-E3JN].

28   [198] *Id.*

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   183.   Oracle intentionally electronically intruded into Dr. Golbeck's home by placing

2 tracking devices on her devices which allowed Oracle to engage in pervasive surveillance of Dr.

3 Golbeck's activities taking place on her devices, within the physical confines of her home. Such

4 conduct is the equivalent of employing an electronic listening device or "bug" within a person's

5 home to surreptitiously monitor aural conversations. That Oracle used its surveillance methods to

6 monitor Dr. Golbeck's communications over the internet, while she was in her home, makes it no

7 less intrusive of her private quarters.

8   184.   Oracle's conduct is outrageous and intolerable in a civilized community.

9 Systematic and ongoing surveillance is unacceptable under Florida law, and Oracle's

10 comprehensive surveillance of Florida Class members has been repeatedly singled out as

11 unacceptable by legislators, the FTC, and others, as described above at paragraphs 162-165. The

12 outrageousness of Oracle's conduct is compounded by Oracle's compiling of profiles of Florida

13 Class members using information collected through systematic surveillance, and selling that

14 information to unknown third parties for profit, as described above.

15   185.   Dr. Golbeck and Florida Class members maintain a reasonable expectation of

16 privacy in the conduct of their lives, including their Internet browsing activities and in their

17 electronic communications and exchange of personal data. The reality of modern life increasingly

18 requires that much of our daily activities are conducted online—Dr. Golbeck and Florida Class

19 members have no practical choice or ability but to conduct their daily lives substantially in the

20 digital world, connected to the Internet. The necessary engagement with the digital world makes

21 Dr. Golbeck's and Florida Class members' private lives susceptible to unlawful observation and

22 recording that is capable of yielding a comprehensive and intrusive chronicle of Plaintiff's and

23 Florida Class members' lives. If Dr. Golbeck's and Florida Class members do not have reasonable

24 expectation of privacy in the conduct of their lives online and the digital transmission of their

25 personal data, they can have no reasonable expectation of privacy for virtually any facet of their

26 lives.

27

28

1   186.   Oracle, in violation of Dr. Golbeck and Florida Class members' reasonable

2   expectation of privacy, intercepts, collects, tracks and compiles their web browsing activity and

3   communications.

4   187.   The nature and volume of the web browsing data collected is such that Oracle's

5   practice of compiling dossiers based on the data it collects violates Dr. Golbeck and Florida Class

6   members' reasonable expectation of privacy. Technological advances, such as Oracle's use of

7   cookies, pixels, and other means to track and compile internet browsing activity, electronic

8   purchases, and electronic communications, provide Oracle with the means to assemble a

9   comprehensive chronicle of Dr. Golbeck and Florida Class members' lives heretofore unseen.

10   Oracle collects and compiles personal information such as Plaintiffs' and Florida Class members'

11   email addresses, location data, and web browsing information, including that relating to race,

12   religion, sexual orientation, and health.

13   188.   Oracle also collects and analyzes Dr. Golbeck and Florida Class members' real-

14   world offline activity, including activities like brick-and-mortar store purchases and location

15   information extracted from their cell phones, and compiles computerized records of those

16   activities. Plaintiffs and Florida Class members do not and cannot know which specific real-world

17   offline activities Oracle may or may not be collecting and analyzing and adding to the digital

18   dossiers it compiles on them.

19   189.   Oracle's conduct as described herein is highly offensive to a reasonable person and

20   constitutes, specifically including the following:

21   a.   Oracle engages in dragnet-style collection and interception of Dr. Golbeck

22   and Florida Class members' Internet activity taking place through their private electronic devices,

23   including their communications with websites, thereby learning intimate details of their daily

24   lives based on the massive amount of information collected about them.

25   b.   Oracle also collects minute details about Dr. Golbeck's and Florida Class

26   members' *offline* activities, including their brick-and-mortar purchases and location information

27   extracted from their cell phones. By its very nature, Plaintiffs and Florida Class members cannot

28   be aware of or consent to this conduct.

- 76 -

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   c.   Oracle creates dossiers based on this online and offline data.

2   190.   Oracle's amassing of the electronic information reflecting all aspects of Dr.

3 Golbeck's and Florida Class members' lives into dossiers for future or present use is in and of

4 itself a violation of Dr. Golbeck's and Florida Class members' right to privacy in light of the

5 serious risk these dossiers pose to their autonomy. Additionally, those dossiers are and can be

6 used to further invade Dr. Golbeck's and Florida Class members' privacy, by, inter alia, allowing

7 third parties to learn intimate details of Plaintiffs' and Florida Class members' lives, and target

8 them for advertising, political, and other purposes, as described herein, thereby harming them

9 through the abrogation of their autonomy and their ability to control the dissemination and use of

10 information about them. Additionally, as described above, the social harms posed by Oracle's

11 conduct impair not only individual autonomy, but the collective autonomy of Florida Class

12 members, whose autonomy is essential to the proper functioning of democratic republics.

13   191.   Dr. Golbeck's privacy interests have been harmed by Oracle's indiscriminate

14 collection and sale of her internet activity, her geolocation information, and her real world

15 activities and purchases.

16   192.   Oracle has violated Dr. Golbeck's and Florida Class members' reasonable

17 expectation of privacy via Oracle's review, analysis, dissemination, and subsequent uses of Dr.

18 Golbeck's and Florida Class members' private and other browsing activity through Oracle's Data

19 Cloud, ID Graph, and Data Marketplace.

20   193.   Oracle lacks a legitimate business interest in stockpiling and compiling the personal

21 information of Dr. Golbeck and Florida Class members.

22   194.   Dr. Golbeck and Florida Class members have been damaged by Oracle's invasion

23 of their privacy and are entitled to just compensation and injunctive relief.

24   195.   As a result of Oracle's actions, Dr. Golbeck and Florida Class members seek

25 injunctive relief, in the form of Oracle's cessation of tracking practices in violation of Dr.

26 Golbeck's and Florida Class members' rights, and destruction of all personal data obtained in

27 violation of Dr. Golbeck's and Florida Class members' rights.

28

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   196.   As a result of Oracle's actions, Dr. Golbeck's and Florida Class members seek

2   nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Florida Class

3   members seek punitive damages because Defendants' actions—which were malicious, oppressive,

4   willful— were calculated to injure Dr. Golbeck and made in conscious disregard Dr. Golbeck's

5   rights. Punitive damages are warranted to deter Oracle from engaging in future misconduct.

6   197.   Dr. Golbeck and Florida Class members seek restitution for the unjust enrichment

7   obtained by Defendants as a result of unlawfully collecting their personal data. These intrusions

8   are highly offensive to a reasonable person. Further, the extent of the intrusion cannot be fully

9   known, as the nature of privacy invasion involves sharing Dr. Golbeck's and Florida Class

10   members' personal information with potentially countless third parties, known and unknown, for

11   undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly

12   offensive nature of Oracle's conduct is the fact that Oracle's principal goal was to surreptitiously

13   monitor Dr. Golbeck and Florida Class members and to allow third parties to do the same.

Fourth Cause of Action
Violation of the California Invasion of Privacy Act
(on behalf of the CIPA Sub-Class)

16   198.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

17   199.   The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code

18   §§ 630 to 638. The Act begins with its statement of purpose:

19   The Legislature hereby declares that advances in science and technology have led
     to the development of new devices and techniques for the purpose of
20   eavesdropping upon private communications and that the invasion of privacy
     resulting from the continual and increasing use of such devices and techniques has
21   created a serious threat to the free exercise of personal liberties and cannot be
     tolerated in a free and civilized society.
22

23   200.   California Penal Code § 631(a) provides, in pertinent part:

24   Any person who, by means of any machine, instrument, or contrivance, or in any
     other manner . . . willfully and without the consent of all parties to the
25   communication, or in any unauthorized manner, reads, or attempts to read, or to
     learn the contents or meaning of any message, report, or communication while the
26   same is in transit or passing over any wire, line, or cable, or is being sent from, or
     received at any place within this state; or who uses, or attempts to use, in any
27   manner, or for any purpose, or to communicate in any way, any information so
     obtained, or who aids, agrees with, employs, or conspires with any person or
     persons to lawfully do, or permit, or cause to be done any of the acts or things
28

1

2

mentioned above in this section, is punishable by a fine not exceeding two
thousand five hundred dollars . . . .

Under either section of the CIPA, a defendant must show it had the consent of all parties to a

3

communication.

4

5

201.   Oracle utilizes a proprietary software device, referred to as "bk-coretag.js"

6

JavaScript code, to "extract," or intercept, "user attributes," which include the contents of users'

7

communications with websites, and secretly sends them to Oracle while the users are in the

8

process of communicating with those websites. Oracle's technical documentation explains that

9

bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views,

10

purchase intent, [and] add-to-cart actions"[199] and other communications that users have with

11

websites and simultaneously copies and sends those communications to Oracle.

12

202.   Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices

13

when they browse a website that contains certain Oracle code. Oracle uses the bk-coretag.js

14

JavaScript code to intercept the contents of Internet users' communications with websites as

15

described at paragraphs 44-50 above. At all relevant times, Oracle's tracking and interceptions of

16

Plaintiff Katz-Lacabe's and CIPA Sub-Class members' internet communications was without

17

authorization and consent from Plaintiff Katz-Lacabe and CIPA Sub-Class members. The

18

interception by Oracle in the aforementioned circumstances were unlawful and tortious.

19

203.   The communications intercepted by Oracle include "contents" of electronic

20

communications made from Plaintiffs Katz-Lacabe and CIPA Sub-Class members to websites

other than those operated by Oracle in the form of:

21

a.   the URLs being browsed by the Internet user as well as the referrer URL;

22

b.   webpage title;

23

c.   webpage keywords;

24

d.   "product page visits"

25

e.   "purchase intent" signals;

26

27

28

---

[199] *Oracle Data Cloud Core Tag Implementation*, Oracle, https://docs.oracle.com/en/cloud/saas/
data-cloud/data-cloud-help-center/IntegratingBlueKaiPlatform/DataIngest/
coretag_implementation.html [https://perma.cc/8XVU-8Z2F].

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   f.   "add-to-cart actions"; and

2   g.   data entered by the user into forms on the website.

3   204.   The URLs being browsed by the Internet user as well as the referrer URL and data

4 entered by the user into forms on the website constitute contents of communications. "Product

5 page visits", "purchase intent" signals;" "add-to-cart actions"; and keywords also constitute

6 contents of communications.[200] These actions communicate the user's intent to a website; for

7 example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and

8 asking to put that book on hold. There is no question that a wiretap of such a phone conversation

9 would intercept the "contents" of a communication. Actions demonstrating purchase intent on

10 websites are no different.

11   205.   On information and belief, Oracle intercepted detailed URLs of webpages Plaintiff

12 Katz-Lacabe viewed, including URLs revealing searches Plaintiff performed, the information

13 Plaintiff entered into forms, including searches for specific content, and communications with

14 websites related to purchases or intended purchases, including product page visits, purchase intent

15 signals and add-to-cart actions. Examples of webpages that Plaintiff Katz-Lacabe interacted with

16 for which the contents of his communications were intercepted by Oracle include, but are not

17 limited, to those listed in paragraph 6 above.

18   206.   Oracle's non-consensual tracking of Plaintiff Katz-Lacabe's and CIPA Sub-Class

19 members' internet communications was designed to attempt to learn at least some meaning of the

20 content in the URLs and other data interception. The URLs being browsed by the Internet user as

21 well as the referrer URL and data entered by the user into forms on the website constitute contents

22

23 [200] Contrary to Oracle's arguments in its Motion to Dismiss Reply brief (*see* Dkt. No. 35 at 13),
Plaintiffs did not and do not concede that information related to product page visits, add-to-cart

24 actions, purchase intent signals, and webpage keywords are not "contents" of communications,
contrary to Oracle's argument in its motion to dismiss briefing. Plaintiffs previously cited cases

25 finding that keywords, add-to-cart actions and similar intent signals and interactions constitute
contents of communications. *See* Motion to Dismiss Opposition (Dkt. No. 30) at 19, citing "*In re*

26 *Google RTB Consumer Priv. Litig.*, 2022 WL 2165489, at *10 ("URL of the page [being
visited]"; "referrer URL that caused navigation to the current page**"; "details about the content**

27 **within the site or app"; and "list of keywords about [the] site or app" constituted "contents"**
of communications for ECPA purposes); *Saleh*, 562 F. Supp. 3d at 518 ("**customer's**

28 **purchasing selections," "keystrokes," and "interactions with" defendants' website were**
contents of communications for ECPA purposes)." (emphasis added).

   SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 of communications. "Product page visits", "purchase intent" signals;" "add-to-cart actions"; and

2 keywords also constitute contents of communications. These actions communicate the user's

3 intent to a website; for example, adding a book to a cart on a website is functionally equivalent to

4 calling a bookstore and asking to put that book on hold. There is no question that a wiretap of such

5 a phone conversation would intercept the "contents" of a communication. Actions demonstrating

6 purchase intent on websites are no different.

7   207. On information and belief, Oracle intercepted detailed URLs of webpages Plaintiff

8 Katz-Lacabe viewed, including URLs revealing searches performed and sensitive content viewed,

9 information Plaintiff Katz-Lacabe entered into forms, including but not limited to searches for

10 specific content, and communications with websites related to purchases or intended purchases,

11 including product page visits, purchase intent signals and add-to-cart actions.

12   208. The following items constitute "machine[s], instrument[s], or contrivance[s]" under

13 the CIPA, and even if they do not, Oracle's deliberate and admittedly purposeful scheme that

14 facilitated its interceptions falls under the broad statutory catch-all category of "any other

15 manner":

16   a. The computer codes and programs Oracle used to track Plaintiffs Katz-

17 Lacabe's and CIPA Sub-Class members' communications, including JavaScript;

18   b. Plaintiffs Katz-Lacabe's and CIPA Sub-Class members' browsers and

19 mobile applications;

20   c. Plaintiffs Katz-Lacabe's and CIPA Sub-Class members' computing and

21 mobile devices;

22   d. The computer codes and programs used by Oracle to effectuate its tracking

23 and interception of the Plaintiffs Katz-Lacabe's and CIPA Sub-Class members'; and

24   e. The plan Oracle carried out to effectuate its tracking and interception of

25 Plaintiffs Katz-Lacabe's and CIPA Sub-Class members' communications.

26   209. Plaintiff Katz-Lacabe and CIPA Sub-Class members have suffered loss by reason

27 of these violations, including, but not limited to, violation of their rights to privacy and loss of

28 value in their personally identifiable information.

- 81 -

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   210.   Pursuant to California Penal Code § 637.2, Plaintiffs Katz-Lacabe and CIPA Sub-

2   Class members have been injured by the violations of California Penal Code § 631, and each seek

3   damages for the greater of $5,000 or three times the amount of actual damages, as well as

4   injunctive relief.

5   **Fifth Cause of Action**
                              Violation of the FSCA, Fla. Stat. Ann. § 934.03
6   **(on behalf of the FSCA Class)**

7   211.   Plaintiff Dr. Golbeck and the FSCA Class members repeat and reallege all

8   preceding paragraphs contained herein.

9   212.   It is a violation of the FSCA to intercept, endeavor to intercept, or procure any

10 other person to intercept or endeavor to intercept any electronic communication. Fla. Stat. Ann.

11 § 934.03(1)(a).

12   213.   Further, it is a violation to intentionally use, or endeavor to use, "the contents of

13 any wire, oral, or electronic communication, knowing or having reason to know that the

14 information was obtained through the interception of a wire, oral, or electronic communication in

15 violation of this subsection[.]" Fla. Stat. Ann. § 934.03(1)(d).

16   214.   The FSCA defines "intercept" as the "acquisition of the contents of any wire,

17 electronic, or oral communication through the use of any electronic, mechanical, or other device."

18 Fla. Stat. Ann. § 934.02(3).

19   215.   Under the FSCA, "contents" includes, but is not limited to, "any information

20 concerning the substance, purport, or meaning of that communication." Fla. Stat. Ann.

21 § 934.02(7).

22   216.   The FSCA defines "electronic communication" as "any transfer of signs, signals,

23 writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a

24 wire, radio, electromagnetic, photoelectronic, or photooptical system that affects intrastate,

25 interstate, or foreign commerce…." Fla. Stat. Ann. § 934.02(12).

26   217.   Oracle utilizes a proprietary software device, referred to as "bk-coretag.js"

27 JavaScript code, to "extract," or intercept, "user attributes," which include the contents of users'

28 communications with websites, and secretly sends them to Oracle while the users are in the

1   process of communicating with those websites. Oracle's technical documentation explains that

2   bk-coretag.js JavaScript code deployed by Oracle collects "user attributes" "such as product views,

3   purchase intent, [and] add-to-cart actions"[201] and other communications that users have with

4   websites and simultaneously copies and sends those communications to Oracle.

5   218.   Oracle places the bk-coretag.js JavaScript code on Internet users' electronic devices

6   when they browse a website that contains certain Oracle code. Oracle uses the bk-coretag.js

7   JavaScript code to intercept the contents of Internet users' communications with websites as

8   described at paragraphs 44–50 above. At all relevant times, Oracle's tracking and interceptions of

9   Plaintiff Golbeck and FSCA Class members' internet communications was without authorization

10   and consent from Dr. Golbeck and FSCA Class members. The interception by Oracle in the

11   aforementioned circumstances were unlawful and tortious.

12   219.   The communications intercepted by Oracle include "contents" of electronic

13   communications made from Dr. Golbeck and FSCA Class members to websites other than those

14   operated by Oracle in the form of:

15   a.   the URLs being browsed by the Internet user as well as the referrer URL;

16   b.   webpage title;

17   c.   webpage keywords;

18   d.   "product page visits"

19   e.   "purchase intent" signals;

20   f.   "add-to-cart actions"; and

21   g.   data entered by the user into forms on the website.

22   220.   The URLs being browsed by the Internet user as well as the referrer URL and data

23   entered by the user into forms on the website constitute contents of communications. "Product

24   page visits" "purchase intent" signals," "add-to-cart actions" and keywords also constitute contents

25   of communications. These actions communicate the user's intent to a website; for example, adding

26

27   [201] *Oracle Data Cloud Core Tag Implementation*, Oracle,
     https://docs.oracle.com/en/cloud/saas/data-cloud/data-cloud-help-
28   center/IntegratingBlueKaiPlatform/DataIngest/coretag_implementation.html
     [https://perma.cc/8XVU-8Z2F].

SECOND AMENDED CLASS ACTION COMPLAINT
                                        CASE NO. 3:22-CV-04792-RS

1 a book to a cart on a website is functionally equivalent to calling a bookstore and asking to put that

2 book on hold. Actions demonstrating purchase intent on websites are "contents" of a

3 communication.

4   221.   On information and belief, Oracle intercepted detailed URLs of webpages Dr.

5 Golbeck viewed, including URLs revealing searches Dr. Golbeck performed, the information Dr.

6 Golbeck entered into forms, including searches for specific content, and communications with

7 websites related to purchases or intended purchases, including product page visits, purchase intent

8 signals and add-to-cart actions. Examples of webpages that Dr. Golbeck interacted with for which

9 the contents of her communications were intercepted by Oracle include, but are not limited, to

10 those listed in paragraphs 14 and 15 above.

11   222.   Oracle's non-consensual tracking of Dr. Golbeck's and FSCA Class members'

12 internet communications was designed to attempt to learn at least some meaning of the content in

13 the URLs and other data interception.

14   223.   The following items constitute "[e]lectronic, mechanical, or other device[s]":

15   a.   The computer codes and programs Oracle used to track Dr. Golbeck and

16 FSCA Class members' communications, including JavaScript;

17   b.   Dr. Golbeck's and FSCA Class members' browsers and mobile

18 applications;

19   c.   Dr. Golbeck's and FSCA Class members' computing and mobile devices;

20   d.   The computer codes and programs used by Oracle to effectuate its tracking

21 and interception of the Plaintiffs Golbeck and FSCA Class members' communications; and

22   224.   The equipment utilized by Oracle to intercept Dr. Golbeck's and the FSCA Class

23 members' electronic communications constitute an apparatus, electronic,

24 or other device under the FSCA as (1) it is not a telephone or telegraph equipment, or any

25 component thereof; and/or (2) it was not furnished to Oracle by a provider of wire or electronic

26 communication services. Fla. Stat. Ann. § 934.02(4). Software constitutes a "device" for purposes

27 of applying wiretap statutes.

28

1   225.   Oracle violated § 934.03(1)(a) of the FSCA by intentionally intercepting Dr.

2   Golbeck and the FSCA Class members electronic communications.

3   226.   Oracle intentionally intercepted Dr. Golbeck's and the FSCA Class members'

4   electronic communications without their prior consent. Oracle used the contents of those

5   communications as described at paragraphs 174-197 above.

6   227.   As a result of Oracle's conduct, and pursuant to § 934.10 of the FSCA, Dr. Golbeck

7   and the FSCA Class members were harmed and are each entitled to "liquidated damages computed

8   at the rate of $100 a day for each day of violation or $1,000, whichever is higher[.]" Fla Stat. Ann.

9   § 934.10(b).

10   228.   Dr. Golbeck and the FSCA Class members are also entitled to "reasonable

11   attorney's fees and other litigation costs reasonably incurred." Fla Stat. Ann. § 934.10(d).

12   229.   Dr. Golbeck and the FSCA Class members are also entitled to an injunction.

13   230.   Dr. Golbeck and the FSCA Class members suffered loss by reason of these

14   violations, including, but not limited to, violation of their rights to privacy.

15
16
<div align="center">

Sixth Cause of Action
Violation of the Federal Wiretap Act, 18 U.S.C. § 2510, et. seq.
(on behalf of the ECPA Class)

</div>

17   231.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

18   232.   The Federal Wiretap Act, as amended by the Electronic Communications Privacy

19   Act of 1986, prohibits the intentional interception of the contents any wire, oral, or electronic

20   communication through the use of a device. 18 U.S.C. § 2511.

21   233.   The Wiretap Act protects both the sending and receipt of communications.

22   234.   18 U.S.C. § 2520(a) provides a private right of action to any person whose "wire,

23   oral, or electronic communication is intercepted, disclosed, or intentionally used "in violation of

24   the Wiretap Act.

25   235.   As described above, Oracle intercepts Plaintiffs Katz-Lacabe's and Golbeck's and

26   ECPA Class members' communications with websites by placing tracking devices, namely the

27   bk-coretag.js JavaScript code, on Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Class

28   members' devices while they are browsing the Internet. This code transmits to Oracle the

1   specific webpages and information about the webpages Plaintiffs Katz-Lacabe and Golbeck and

2   ECPA Class members' are browsing, as well as the other data described herein, which Oracle

3   uses to enrich the dossiers it compiles on Plaintiffs Katz-Lacabe and Golbeck and ECPA Class

4   members.

5   236.   Oracle's actions in intercepting and tracking user communications while they were

6   browsing the internet was intentional. On information and belief, Oracle is aware that it is

7   intercepting communications in these circumstances and has taken no remedial action.

8   237.   Oracle's interception of internet communications that Plaintiffs Katz-Lacabe and

9   Golbeck and ECPA Class members were sending and receiving was done contemporaneously

10   with the sending and receipt of those communications.

11   238.   The communications intercepted by Oracle include "contents" of electronic

12   communications made from Plaintiffs Katz-Lacabe and Golbeck and ECPA Class members to

13   websites other than those operated by Oracle in the form of:

14   a.   the URLs being browsed by the Internet user as well as the referrer URL;

15   b.   webpage title;

16   c.   webpage keywords;

17   d.   "product page visits"

18   e.   "purchase intent" signals;

19   f.   "add-to-cart actions"; and

20   g.   data entered by the user into forms on the website.

21   239.   The URLs being browsed by the Internet user as well as the referrer URL and data

22   entered by the user into forms on the website constitute contents of communications. "Product

23   page visits", "purchase intent" signals;" "add-to-cart actions"; and keywords also constitute

24   contents of communications. These actions communicate the user's intent to a website; for

25   example, adding a book to a cart on a website is functionally equivalent to calling a bookstore and

26   asking to put that book on hold. There is no question that a wiretap of such a phone conversation

27   would intercept the "contents" of a communication. Actions demonstrating purchase intent on

28   websites are no different.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   240.   On information and belief, Oracle intercepted detailed URLs of web pages

2   Plaintiffs viewed, including URLs revealing searches Plaintiffs performed, the information

3   Plaintiffs entered into forms, including searches for specific content, and communications with

4   websites related to purchases or intended purchases, including product page visits, purchase intent

5   signals and add-to-cart actions.

6   241.   The transmission of data between Plaintiffs Katz-Lacabe and Golbeck and ECPA

7   Class members on the one hand and the websites on which Oracle tracked and intercepted their

8   communications on the other, without authorization were "transfer[s] of signs, signals, writing, . .

9   . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio,

10   electromagnetic, photoelectronic, or photooptical system that affects interstate commerce[,]" and

11   were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

12   242.   The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

13   a.   The computer codes and programs Oracle used to track Plaintiffs Katz-

14   Lacabe's and Golbeck's and ECPA Class members' communications, including JavaScript code;

15   b.   Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Class members'

16   browsers and mobile applications;

17   c.   Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Class members'

18   computing and mobile devices;

19   d.   The computer codes and programs used by Oracle to effectuate its tracking

20   and interception of the Plaintiffs' and ECPA Class members' communications; and

21   e.   The plan Oracle carried out to effectuate its tracking and interception of the

22   Plaintiffs Katz-Lacabe's and Golbeck's and ECPA Class members' communications while

23   browsing the internet.

24   243.   Oracle, in its conduct alleged here, was not providing an "electronic

25   communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in

26   the Wiretap Act. Oracle was not acting as an Internet Service Provider (ISP).

27   244.   Oracle was not an authorized party to the communication because Plaintiffs Katz-

28   Lacabe and Golbeck and ECPA Class members were unaware of Oracle's interception of their

1   communications with websites, and did not knowingly send any communication to Oracle. Oracle

2   could not manufacture its own status as a party to Plaintiffs Katz-Lacabe's and Golbeck's and

3   ECPA Class members' communications with others by surreptitiously intercepting those

4   communications.

5   245.   As described above, the communications between Plaintiffs Katz-Lacabe and

6   Golbeck and ECPA Class members on the one hand, and websites on the other, were

7   simultaneous to, but *separate* from, the channel through which Oracle acquired the contents of

8   those communications.

9   246.   The interception by Oracle in the aforementioned circumstances was performed for

10   the secondary and independent purpose of committing tortious acts in violation of the law,

11   specifically:

12   a.   Violating the California Constitution's prohibition on the compiling of

13   electronic dossiers, which dossiers are enriched by the contents of the communications

14   intercepted by Oracle, as described herein;

15   b.   Violating the tort of intrusion upon seclusion by using the contents of the

16   intercepted communications to create detailed profiles on Plaintiffs Katz-Lacabe and Golbeck and

17   ECPA Class members, and then making those profiles available through Oracle's Data Cloud, ID

18   Graph, and Data Marketplace, as described herein;

19   247.   On information and belief, and as described above in detail at Section VI.F., Oracle

20   was aware that its conduct of profiling ECPA Class members was tortious and intended to violate

21   ECPA Class members' privacy and other rights.

22   248.   Parties knowingly engaged in tortious conduct such as blackmail, theft of business

23   secrets, or the misappropriation of a person's identity, primarily intend to "make money" through

24   that conduct. The goal of making money through advertising revenue does not sanitize the

25   intentional commission of a tort by Oracle. The mere existence of a lawful purpose alone does not

26   "sanitize a[n interception] that was also made for an illegitimate purpose." *Sussman v. ABC*, 186

27   F.3d 1200, 1202 (9th Cir.1999), cert denied, 528 U.S. 1131 (2000). The 1) compiling of electronic

28   dossiers, which dossiers are enriched by the contents of the communications intercepted by Oracle

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 in violation of the California Constitution, 2) use of the contents of the intercepted

2 communications to create detailed profiles on ECPA Class members and then make those profiles

3 available through Oracle's Data Cloud, ID Graph, and Data Marketplace, in violation the tort of

4 intrusion upon seclusion, are tortious and illegitimate purposes under the ECPA.

5   249.   Consent is not a defense where a "communication is intercepted for the purpose of

6 committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Subsequent disclosure of the

7 contents of the intercepted conversations for the purpose of further invading the Plaintiffs' privacy

8 is a tortious act that satisfies this exception to consent. In addition to having the intent of profiting

9 from the sale of Plaintiffs' personal information, Oracle knowingly and intentionally invaded

10 Plaintiffs' privacy through intercepting their communications, compiling those communications

11 into dossiers for sale, and then sharing the contents of those communications with third parties.

12 Any disputes as to Oracle's intent under the wiretapping statute are to be decided by the jury.

13   250.   Oracle intercepted Plaintiffs' communications for the purpose of associating their

14 data with preexisting profiles, and as such a primary motivation or determining factor in Oracle's

15 actions has been to injure Plaintiffs tortiously. The association of Plaintiffs' data with preexisting

16 user profiles, as described herein (*see, e.g*., paragraphs 4-10, 11-19 41-71, *supra*), is a further use

17 of Plaintiffs' data that satisfies the 'exception to the exception.' Section 2511 applies where the

18 recording is done for the purpose of facilitating some further impropriety, and recognized tortious

19 purposes providing a basis for the 'exception to the exception' include facilitating invading a

20 plaintiff's privacy. The exception applies where subsequent disposition of the fruits of the

21 interception constitute the further tortious act.

22   251.   After intercepting the communications, Oracle then used the contents of the

23 communications knowing or having reason to know that such information was obtained through

24 the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

25   252.   As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may

26 assess statutory damages to Plaintiffs Katz-Lacabe and Golbeck and ECPA Class members;

27 injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but

28

1   sufficient to prevent the same or similar conduct by Oracle in the future, and a reasonable

2   attorney's fees and other litigation costs reasonably incurred.

3   **Seventh Cause of Action**
                   Unjust Enrichment under California Common Law
4   **(on behalf of the California Class)**

5   253.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

6   254.   Plaintiffs allege unjust enrichment under California law on behalf of the California

7   Class.

8   255.   Oracle has wrongfully and unlawfully trafficked in the named Plaintiffs' and

9   California Class members' personal information and other personal data without their consent for

10   substantial profits.

11   256.   Plaintiffs' and California Class members' personal information and data have

12   conferred an economic benefit on Oracle.

13   257.   Oracle has been unjustly enriched at the expense of Plaintiffs and California Class

14   members, and the company has unjustly retained the benefits of its unlawful and wrongful

15   conduct.

16   258.   It would be inequitable and unjust for Oracle to be permitted to retain any of the

17   unlawful proceeds resulting from its unlawful and wrongful conduct.

18   259.   Plaintiffs and California Class members accordingly are entitled to equitable relief

19   including restitution and disgorgement of all revenues, earnings, and profits that Oracle obtained

20   as a result of its unlawful and wrongful conduct.

21   260.   When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff

22   may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no

23   corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of

24   legally protected rights that enriched a defendant. Oracle has been unjustly enriched by virtue of

25   its violations of Plaintiffs' and California Class members' legally protected rights to privacy as

26   alleged herein, entitling Plaintiffs and California Class members to restitution of Oracle's

27   enrichment. "[T]he consecrated formula 'at the expense of another' can also mean 'in violation of

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                                       CASE NO. 3:22-CV-04792-RS

1 the other's legally protected rights,' without the need to show that the claimant has suffered a loss."

2 Restatement (Third) of Restitution § 1, cmt. a.

3   261.   The elements for a claim of unjust enrichment are (1) receipt of a benefit and (2)

4 unjust retention of the benefit at the expense of another. The doctrine applies where plaintiffs,

5 while having no enforceable contract, nonetheless have conferred a benefit on defendant which

6 defendant has knowingly accepted under circumstances that make it inequitable for the defendant

7 to retain the benefit without paying for its value.

8   262.   It is a longstanding principle of law embodied in the Restatement (Third) of

9 Restitution and Unjust Enrichment (2011) that a person who is unjustly enriched at the expense of

10 another may be liable for the amount of the unjust enrichment even if the defendant's actions

11 caused the plaintiff no corresponding loss. Where "a benefit has been received by the defendant

12 but the plaintiff has not suffered a corresponding loss or, in some cases, any loss, but nevertheless

13 the enrichment of the defendant would be unjust ... [t]he defendant may be under a duty to give to

14 the plaintiff the amount by which [the defendant] has been enriched." Rest., Restitution, § 1, com.

15 e.

16   263.   The comments to the Restatement (Third) explicitly recognize that an independent

17 claim for unjust enrichment may be predicated on a privacy tort. Restatement (Third) of

18 Restitution and Unjust Enrichment § 44 cmt. b ("Profitable interference with other protected

19 interests, such as the claimant's right of privacy, gives rise to a claim under § 44 if the benefit to

20 the defendant is susceptible of measurement").

21   264.   Moreover, the Restatement recognizes that in the context of a privacy violation, the

22 claimant need not be in direct privity with the wrongdoer, and likewise, California law imposes no

23 requirement of privity to make out an unjust enrichment claim. The Restatement comments

24 provide the following illustrative example:

25   10. On going out of business, Local Pharmacy sells Customers' prescription
                records and accompanying medical information to National Chain. In
26   connection with the sale, Local Pharmacy agrees not to inform Customers
                of the pending disclosure of their records; the object of this provision is to
27   allow National Chain to communicate with Customers once their files have
                been transferred. Because it gives Customers no opportunity to object to

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

1
2
3
4
5

the disclosure of confidential information, the transaction between Local
Pharmacy and National Chain is both a violation of Customers' protected
right of privacy in their prescription records and a deceptive marketing
practice under local law. By the rule of this section, Customers have a
claim against Local Pharmacy for the proceeds of the sale of their
confidential information*, and a claim against National Chain for the
additional profits it derived from the unlawful transaction.*" *Id*. § 44 cmt. b,
illus. 10 (emphasis added).

6
7
8
9
10
11

265.   Because "[a] person is not permitted to profit by his own wrong," *id.* § 3, "[g]ains

realized by misappropriation, or otherwise in violation of another's legally protected rights, must

be given up to the person whose rights have been violated." *Id.* ch. 5, introductory note. These

principles are deeply ingrained in California law. California courts have long recognized a

common law claim based on unjust enrichment. In determining the remedy for such claims,

California courts apply principles found in the Restatement.

12
13
14
15
16
17
18
19
20
21
22
23
24

266.   California law recognizes a right to disgorgement of profits resulting from unjust

enrichment, even where an individual has not suffered a corresponding loss. The public policy of

California does not permit one to 'take advantage of his own wrong' regardless of whether the

other party suffers actual damage. Where the defendant has been unjustly enriched but the

plaintiff has not proven any monetary loss, the proper remedy is for the defendant to disgorge

those ill-gotten gains. A defendant acting in conscious disregard of the rights of another should be

required to disgorge all profit because disgorgement both benefits the injured parties and deters the

perpetrator from committing the same unlawful actions again. Without this result, there would be

an insufficient deterrent to improper conduct that is more profitable than lawful conduct.

"Restitution requires full disgorgement of profit by a conscious wrongdoer, not just because of the

moral judgment implicit in the rule of this section, but because any lesser liability would provide

an inadequate incentive to lawful behavior." Restatement (Third) of Restitution and Unjust

Enrichment § 3, cmt. b.

25
26
27

267.   The unauthorized use of Plaintiffs' and California Class members' information for

profit entitles them to profits unjustly earned. That is so, moreover, regardless of whether Plaintiffs

28

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1   and California Class members planned to sell their data or whether the individual's data is made

2   less valuable, and regardless of whether Plaintiffs were in privity with Oracle.

3   268.   Oracle has unjustly profited from disclosing users' browsing histories, internet

4   activity, and real world activity to third parties without Plaintiffs' and California Class members'

5   knowledge or consent.

6   269.   A portion—but not all—of the unjust enrichment Oracle obtained was through the

7   use of Plaintiffs' and California Class members' web browsing activities. In addition to data

8   related to web browsing, Oracle collected and sold information regarding Plaintiffs' and California

9   Class members' physical movements through geolocation data, and Plaintiffs' and California Class

10   members' offline purchases and activities, including through credit cards and brick-and-mortar

11   establishments. The combination of this data with Plaintiffs' and California Class members' web

12   browsing and purchase activity constitutes an invasion of privacy. Moreover, the access Plaintiffs

13   and California Class members received to those websites does not defeat their unjust enrichment

14   claim because:

15   a.   As described in Section VI.E. above, Plaintiffs were not aware of Oracle's

16   conduct while browsing websites and did not and could not consent to that conduct. Had

17   Plaintiffs known of Oracle's conduct, Plaintiffs would not have visited those websites or, if such

18   visits were unavoidable, would have taken additional precautions to avoid being tracked and

19   profiled by Oracle. Oracle's conduct with respect to tracking Plaintiffs' conduct on any particular

20   website cannot be viewed in isolation—the aggregation, compilation, analysis, and sale of that

21   extensive information about Plaintiffs' internet viewing habits violates Plaintiffs' California

22   Constitutional and common law rights. Moreover, the fruits of Oracle's illegal wiretapping of

23   Plaintiffs' communications with many websites, in violation of criminal statutes, also contributed

24   to Oracle's enrichment. Oracle's enrichment through violation of criminal wiretapping statutes is

25   inherently unjust.

26   b.   Plaintiffs were not aware of and did not consent to the collection of their

27   location data by Oracle, which is independent of their visit to any website. Oracle was unjustly

28   enriched by the acquisition and sale of Plaintiffs' geolocation data.

SECOND AMENDED CLASS ACTION COMPLAINT
                                                         CASE NO. 3:22-CV-04792-RS

1   c.   Plaintiffs were not aware of and did not consent to the collection of their

2   real-world activity, such as brick-and-mortar purchases, which is independent of their visit to any

3   website. Oracle was unjustly enriched by the acquisition and sale of Plaintiffs' brick-and mortar-

4   purchase data.

5   270.   Plaintiffs did not provide authorization for the use of their personal information, nor

6   did Oracle provide them with control over its use to produce revenue. This unauthorized use of

7   their information for profit entitles Plaintiffs to profits unjustly earned.

8   271.   Plaintiffs' aggregate browsing histories carry financial value. Oracle was unjustly

9   enriched by aggregate Plaintiffs' personal and sensitive data into detailed dossiers that it makes

10   available to third parties.

11   272.   Oracle Advertising, the service which appears to administer the products at issue in

12   this Complaint, had revenue in 2021 alone of approximately $2 billion. An unknown portion of

13   this revenue was generated through the wrongful acquisition and sale of California Class

14   members' data, as described herein. The portion of Oracle's revenue attributable to Oracle's

15   wrongful conduct described herein is susceptible of measurement and can be determined through

16   discovery.

17   273.   A 2019 study co-authored by Robert J. Shapiro and Siddartha Aneja, titled *Who*

18   *Owns America's Personal Information and What is it Worth*?, calculated the value of Americans'

19   personal information gathered and used by various data brokers as follows: $13.3 billion in 2016,

20   $13.8 billion in 2017, and $14.8 billion in 2018.[202]

21   274.   It would be unjust and inequitable to allow Oracle to profit from its violation of the

22   Plaintiffs and California Class members' Constitutional, common law, and statutory rights as

23   described herein. Oracle's conduct in creating cradle-to-grave profiles of Plaintiffs and California

24   Class members is conduct that was specifically singled out for disapprobation by the voters of

25

26   [202] Robert Shapiro and Siddhartha Aneja, *Who Owns Americans' Personal Information and What*
     Is It Worth?, Future Majority (April 2019), available at https://assets.futuremajority.org/uploads/

27   report-for-future-majority-on-the-value-of-people-s-personal-data-shapiro-aneja-march-8-
     2019.pdf. While Oracle was not included in this particular study, on information and belief the

28   value of the information collected and used by Oracle is similar to if not larger than those of the
     data brokers described in the study.

SECOND AMENDED CLASS ACTION COMPLAINT
                                               CASE NO. 3:22-CV-04792-RS

1   California in amending the California Constitution. Oracle's conduct is highly offensive to a

2   reasonable person, and as such, regardless of whether Plaintiffs received anything of value from

3   the websites they visited, Oracle's profiting from its collection and use of their data violates

4   California public policy and goes well beyond acceptable social norms.

5   275.   Oracle was aware of the benefit conferred by Plaintiffs. Oracle CEO Larry Ellison

6   described in detail Oracle's plan to profit from its acquisition and use of California Class

7   members' data. *See* paragraphs 68-71, *supra*. Indeed, Oracle's Data Marketplace is premised

8   entirely on the sale of such data to third parties. Oracle acted in conscious disregard of the rights of

9   Plaintiffs and California Class members and should be required to disgorge all profit obtained

10 therefrom to deter Oracle and others from committing the same unlawful actions again.

11   **Eighth Cause of Action**
     Unjust Enrichment under Florida Law (on behalf of the Florida Class)
12

13   276.   Plaintiffs repeat and reallege all preceding paragraphs contained herein.

14   277.   Plaintiffs allege this claim for Unjust Enrichment under Florida Law on behalf of

15 the Florida Class.

16   278.   There are three elements of an unjust enrichment claim under Florida law: first, the

17 plaintiff has conferred a benefit on the defendant; second, the defendant voluntarily accepted and

18 retained that benefit; and, finally, the circumstances are such that it would be inequitable for the

19 defendants to retain the benefit without paying for it.

20   279.   When a defendant is unjustly enriched at the expense of a plaintiff, the plaintiff

21 may recover the amount of the defendant's unjust enrichment even if plaintiff suffered no

22 corresponding loss, and plaintiff is entitled to recovery upon a showing of merely a violation of

23 legally protected rights that enriched a defendant. Oracle has been unjustly enriched by virtue of

24 its violations of Plaintiff Golbeck's and the Florida Class members' legally protected rights to

25 privacy as alleged herein, entitling Plaintiff Golbeck and the Florida Class members to restitution

26 of Oracle's enrichment.

27

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                                CASE NO. 3:22-CV-04792-RS

1 280. Oracle has wrongfully and unlawfully trafficked in Plaintiff Golbeck's and the

2 Florida Class members' personal information and other personal data without their consent for

3 substantial profits.

4 281. Plaintiff Golbeck's and the Florida Class members' personal information and data

5 have conferred an economic benefit on Oracle. Oracle voluntarily accepted and retained that

6 benefit.

7 282. Oracle has been unjustly enriched at the expense of Plaintiff Golbeck and the

8 Florida Class members, and the company has unjustly retained the benefits of its unlawful and

9 wrongful conduct, as described above. Oracle has violated Dr. Golbeck's right to privacy as well

10 as her rights under the ECPA and the Florida FSCA. It would be inequitable and unjust for Oracle

11 to be permitted to retain any of the unlawful proceeds resulting from its unlawful and wrongful

12 conduct.

13 283. Dr. Golbeck and Florida Class members accordingly are entitled to equitable relief

14 including restitution and disgorgement of all revenues, earnings, and profits Oracle obtained as a

15 result of its unlawful and wrongful conduct.

16 **Ninth Cause of Action**
Declaratory Judgment that Oracle Wrongfully Accessed, Collected, Stored,

17 **Disclosed, Sold, and Otherwise Improperly Used Plaintiffs' Private Data**
and Injunctive Relief

18 **(on behalf of all Classes)**

19 284. Plaintiffs incorporate the substantive allegations contained in all prior and

20 succeeding paragraphs as if fully set forth herein.

21 285. The gravamen of this controversy lies in Oracle's collection, tracking, and analysis

22 of Plaintiffs' and Class members' personal information and behavior, and building dossiers based

23 on that information and providing that information to third parties. Plaintiffs and Class members

24 never consented to, or were even aware of, Oracle's conduct described herein.

25 286. Oracle's misconduct has put Plaintiffs' and Class members' privacy and autonomy

26 at risk, and violated their dignitary rights, privacy, and economic well-being.

27 287. Accordingly, Plaintiffs seek appropriate declaratory relief, and injunctive relief as

28 prayed for below.

SECOND AMENDED CLASS ACTION COMPLAINT
CASE NO. 3:22-CV-04792-RS

1 **IX.   PRAYER FOR RELIEF**

2   WHEREFORE, Plaintiffs respectfully request that this Court:

3   A.   Issue an order determining that this action may be maintained as a class action

4 under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class

5 representatives, that Plaintiffs' attorneys shall be appointed as Class counsel pursuant to Rule

6 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

7   B.   Certify this action is a class action pursuant to Rule 23 of the Federal Rules of

8 Civil Procedure;

9   C.   Appoint Plaintiffs to represent the Classes;

10   D.   Appoint undersigned counsel to represent the Classes;

11   E.   Enter Judgment in favor of Plaintiffs and the members of the Class against Oracle

12 awarding damages, including punitive damage, and/or nominal damages, to Plaintiffs and the

13 Class members, in an amount according to proof at trial, including interest thereon;

14   F.   Enter Judgment in favor of Plaintiffs and the members of the Class against Oracle

15 awarding unjust enrichment and/or restitution of Oracle's ill-gotten gains, revenues, earnings, or

16 profits that it derived, in whole or in part, from its unlawful collection and use of Class members'

17 personal data, in an amount according to proof at trial;

18   G.   Enter Declaratory Judgment in favor of Plaintiffs and the members of the Class

19 against Oracle pursuant to 28 U.S.C. § 2201, declaring that Oracle's conduct is unlawful as

20 alleged herein.

21   H.   Permanently restrain Oracle, and its officers, agents, servants, employees and

22 attorneys, from intercepting, tracking, collecting, or compiling the personal information of Class

23 members as alleged herein;

24   I.   Award Plaintiffs and the Class members their reasonable costs and expenses

25 incurred in this action, including attorneys' fees and expert fees; and

26   J.   Grant Plaintiffs and the Class members further equitable, injunctive, declaratory,

27 or other relief as the Court deems appropriate.

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS

1   **X.   DEMAND FOR JURY TRIAL**

2   Plaintiffs hereby demand a trial by jury of all issues so triable.

3

4   Dated: November 17, 2023   Respectfully Submitted,

5   */s/ Michael W. Sobol*

6   Michael W. Sobol (SBN 194857)
                                          msobol@lchb.com
7   David T. Rudolph (SBN 233457)
                                          drudolph@lchb.com
                                          Jallé H. Dafa (SBN 290637)
8   jdafa@lchb.com
                                          John D. Maher (SBN 316157)
9   jmaher@lchb.com
                                          Nabila Abdallah (SBN 347764)
10   nabdallah@lchb.com
                                          LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
11   275 Battery Street, 29th Floor
                                          San Francisco, CA 94111-3339
12   Telephone: 415.956.1000
                                          Facsimile: 415.956.1008

13   *Attorneys for Plaintiffs and the Class*

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

SECOND AMENDED CLASS ACTION COMPLAINT
                                          CASE NO. 3:22-CV-04792-RS